An analysis of digital forensic units

Kaitlyn Gurule

Purdue University

Follow this and additional works at: https://docs.lib.purdue.edu/open_access_theses

Recommended Citation

https://docs.lib.purdue.edu/open_access_theses/948

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.
This is to certify that the thesis/dissertation prepared

By  Kaitlyn Gurule

Entitled
AN ANALYSIS OF DIGITAL FORENSIC UNITS

For the degree of  Master of Science

Is approved by the final examining committee:

Dr. Kathryn Seigfried-Spellar  5/12/2016
Chair
Dr. Marcus K. Rogers  5/12/2016
Lonnie Bentley  5/12/2016

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University’s “Policy of Integrity in Research” and the use of copyright material.

Approved by Major Professor(s):  Dr. Kathryn Seigfried-Spellar

Approved by:  Jeffrey Whitten  5/12/2016
Head of the Departmental Graduate Program  Date
AN ANALYSIS OF DIGITAL FORENSIC UNITS

A Thesis
Submitted to the Faculty
of
Purdue University
by
Kaitlyn Gurule

In Partial Fulfillment of the
Requirements for the Degree
of
Master of Science

August 2016
Purdue University
West Lafayette, Indiana
To my mother and my father.
Thank you for always believing in me and pushing me to do my best and be the
best in all I do.
ACKNOWLEDGMENTS

First and foremost, I’d like to thank my mother and father for all the guidance and support you have given me. I could not have gotten to where I am today without you. The opportunities you have given me are invaluable and I will always be grateful. To my brother and sisters thank you for always pushing me and helping me to believe in myself. To the rest of my family and friends, thank you for everything you have done to support me along my journey and helping me to follow my dreams.

To Dr. Kathryn Seigfried-Spellar, thank you for the insight, guidance, support and inspiration during this study. This study would not have been half as good without your feedback. You are an amazing professor and I am so glad to have had the opportunity to work with you.

To Dr. Marcus Rogers, thank you for coming to Sandia National Labs (when I was a freshman in undergraduate school) and motivating me to pursue a career in computer forensics. Your motivation led me to attend Purdue and study an amazing field. You have been a great professor to work with.

To Mr. Lonnie Bentley, thank you for helping me with this project and showing me how I can use this information to develop a unit of my own one day.

To everyone else (there are too many to name) who have offered advice or motivation. You have all helped me to reach my goals and I can’t thank you enough.

I’d also like to thank each of the participating units and the unit members who so willingly provided their valuable time to answer my questions. I hope this research will help and be beneficial to you!
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF TABLES</td>
<td>vi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>viii</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>ix</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>xi</td>
</tr>
<tr>
<td>CHAPTER 1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Scope</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Significance</td>
<td>2</td>
</tr>
<tr>
<td>1.3 Research Question</td>
<td>3</td>
</tr>
<tr>
<td>1.4 Assumptions</td>
<td>3</td>
</tr>
<tr>
<td>1.5 Limitations</td>
<td>3</td>
</tr>
<tr>
<td>1.6 Delimitations</td>
<td>4</td>
</tr>
<tr>
<td>1.7 Summary</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 2. REVIEW OF RELEVANT LITERATURE</td>
<td>5</td>
</tr>
<tr>
<td>2.1 The Evolution and History of Digital Forensics</td>
<td>5</td>
</tr>
<tr>
<td>2.2 Cyberforensic Process Models</td>
<td>8</td>
</tr>
<tr>
<td>2.3 A Growing Problem</td>
<td>11</td>
</tr>
<tr>
<td>2.4 Challenges in Cyberforensics &amp; Law Enforcement</td>
<td>15</td>
</tr>
<tr>
<td>2.5 Cyberforensics Laboratories</td>
<td>17</td>
</tr>
<tr>
<td>2.6 Summary</td>
<td>18</td>
</tr>
<tr>
<td>CHAPTER 3. FRAMEWORK AND METHODOLOGY</td>
<td>19</td>
</tr>
<tr>
<td>3.1 Hypothesis</td>
<td>19</td>
</tr>
<tr>
<td>3.2 Unit &amp; Sampling</td>
<td>20</td>
</tr>
<tr>
<td>3.2.1 Sample</td>
<td>20</td>
</tr>
<tr>
<td>3.2.2 Data Retrieval</td>
<td>20</td>
</tr>
<tr>
<td>3.2.3 Comparative Analysis</td>
<td>23</td>
</tr>
<tr>
<td>3.3 Summary</td>
<td>24</td>
</tr>
<tr>
<td>CHAPTER 4. RESULTS</td>
<td>25</td>
</tr>
<tr>
<td>4.1 Unit Descriptives</td>
<td>26</td>
</tr>
<tr>
<td>4.1.1 Setup of the Unit</td>
<td>26</td>
</tr>
<tr>
<td>4.2 Hypothesis Testing</td>
<td>29</td>
</tr>
</tbody>
</table>
### LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Dollar Loss Per State Reported to IC3</td>
<td>13</td>
</tr>
<tr>
<td>2.2 Number of Complaints Reported to IC3</td>
<td>14</td>
</tr>
<tr>
<td>4.1 Generalized Geographical Location of Participating Units</td>
<td>26</td>
</tr>
<tr>
<td>4.2 Cybercrime Unit Structure</td>
<td>28</td>
</tr>
<tr>
<td>4.3 Number of Cases Among the Units</td>
<td>30</td>
</tr>
<tr>
<td>4.4 Types of Digital Evidence Processed Before and After the Unit Was Created</td>
<td>32</td>
</tr>
<tr>
<td>4.5 Backlog Among the Units</td>
<td>34</td>
</tr>
<tr>
<td>4.6 Time Spent to Close Cases</td>
<td>35</td>
</tr>
<tr>
<td>4.7 Cybercrime Unit Funding</td>
<td>36</td>
</tr>
<tr>
<td>4.8 Cybercrime Unit Certifications</td>
<td>38</td>
</tr>
<tr>
<td>4.9 Number of Units Working on Federal, State and Local Cases.</td>
<td>41</td>
</tr>
<tr>
<td>4.10 Number of Units Working on Specific Types of Crimes.</td>
<td>42</td>
</tr>
<tr>
<td>4.11 Average Percentage of Time Spent On Specific Crimes</td>
<td>43</td>
</tr>
<tr>
<td>4.12 Types of Digital Forensics Involved in the Cases</td>
<td>44</td>
</tr>
<tr>
<td>4.13 Number of NCMEC Leads and IC3 Reports</td>
<td>45</td>
</tr>
<tr>
<td>4.14 Successful Unit</td>
<td>46</td>
</tr>
<tr>
<td>4.15 Unit Creation Recommendation</td>
<td>47</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Shows different digital forensic process models with both similar and distinct steps. Adapted from “Digital Evidence And Computer Crime: Forensic Science, Computers and the Internet (Third ed.) p. 189. Copyright 2011 by Elsevier Inc.”</td>
<td>9</td>
</tr>
<tr>
<td>4.1</td>
<td>Shows the number of units working on federal, state and local cases.</td>
<td>40</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>ACE</td>
<td>AccessData Certified Examiner</td>
<td></td>
</tr>
<tr>
<td>ADFM</td>
<td>Abstract Digital Forensics Model</td>
<td></td>
</tr>
<tr>
<td>ASCLD</td>
<td>American Society of Crime Lab Directors</td>
<td></td>
</tr>
<tr>
<td>CART</td>
<td>Computer Analysis and Response Team</td>
<td></td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
<td></td>
</tr>
<tr>
<td>EIDIP</td>
<td>Enhanced Digital Investigation Process Model</td>
<td></td>
</tr>
<tr>
<td>EnCE</td>
<td>EnCase Certified Examiner</td>
<td></td>
</tr>
<tr>
<td>ENIAC</td>
<td>Electronic Numerical Integrator And Computer</td>
<td></td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
<td></td>
</tr>
<tr>
<td>FTK</td>
<td>Forensic Toolkit</td>
<td></td>
</tr>
<tr>
<td>GIAC</td>
<td>Global Information Assurance Certification</td>
<td></td>
</tr>
<tr>
<td>HOBFDIP</td>
<td>Hierarchical Objectives-based Framework for Digital Investigations Process</td>
<td></td>
</tr>
<tr>
<td>IACIS</td>
<td>International Association of Computer Investigative Specialists</td>
<td></td>
</tr>
<tr>
<td>IC3</td>
<td>Internet Crime Complaint Center</td>
<td></td>
</tr>
<tr>
<td>IDIP</td>
<td>Integrated Digital Investigation Model</td>
<td></td>
</tr>
<tr>
<td>NCMEC</td>
<td>National Center for Missing &amp; Exploited Children</td>
<td></td>
</tr>
<tr>
<td>NIJ</td>
<td>National Institute of Justice</td>
<td></td>
</tr>
<tr>
<td>RCFL</td>
<td>Regional Computer Forensics Laboratory</td>
<td></td>
</tr>
<tr>
<td>SCERS</td>
<td>Seized Computer Evidence Recovery Specialist</td>
<td></td>
</tr>
<tr>
<td>SWGDE</td>
<td>Scientific Working Group on Digital Evidence</td>
<td></td>
</tr>
</tbody>
</table>
## Glossary

**Byte**  
A byte is a group of 8 bits, also called a character. Computer storage space is measured in bytes. A kilobyte represents 1000 bytes, a megabyte represents 1000 KB, a gigabyte represents 1000 MB, and a terabyte represents 1000 GB (Oualline, 1997).

**Computer Forensics**  
Also known as cyberforensics, is the preservation, identification, extraction, documentation, and interpretation of computer media for evidence of criminal acts (Kruse & Heiser, 2002).

**Cybercrime**  
Also known as computer crime or digital crime, is a crime that utilizes computer technology to commit crimes (Clifford, 2011).

**Cyberspace**  
The virtual environment (Clifford, 2011).

**Cyberstalking**  
The use of digital media to harass or threaten another person (Easttom, 2014).

**Digital Evidence**  
Information that has been processed and analyzed to determine the relevant data for an investigation that supports or refutes investigative findings (Easttom, 2014).

**Digital Forensics**  
The analysis of digital evidence which includes network forensics, computer forensics, mobile device forensics and malware forensics (Casey, 2011).

**Fraud**  
Any attempt to gain financial reward through deception (Easttom, 2014).
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>The worldwide network of networks which use the TCP/IP protocol to facilitate information exchange (Kroll Ontrack, 2015).</td>
</tr>
<tr>
<td>Mobile Forensics</td>
<td>The process of searching the contents of cell phones (Easttom, 2014).</td>
</tr>
<tr>
<td>Network</td>
<td>A group of computers or devices that is connected together for the exchange of data and sharing of resources (Kroll Ontrack, 2015).</td>
</tr>
</tbody>
</table>
ABSTRACT

Gurule, Kaitlyn M.S., Purdue University, August 2016. An Analysis of Digital Forensic Units. Major Professor: Kathryn Seigfried-Spellar.

Technology is growing rapidly. The first computer, ENIAC, was built in 1946 and it was not until 1975 that personal computers existed (Knight, 2014). Now, computers are seen everywhere. It is rare to see a person without a computer, such as a mobile phone. As technology grows so does computer crimes. Computer crimes, for the purposes of this study, are crimes committed using digital media as a target of a crime, to assist in a crime, or as an incidental element in a crime. Criminals are taking advantage of the new technology and using it to their advantage. Easy access to technology makes it easier for criminals to commit new and old crimes. Law Enforcement agencies are having a difficult time processing all the digital media in an effective and efficient manner. Criminals, however, do not stop committing crimes. Therefore, creating a backlog of cases for law enforcement investigators. Technology creates a variety of difficulties that law enforcement agencies must overcome to successfully process digital media. In order to help overcome these difficulties, some states have created specialized and non-specialized cybercrime units. These cybercrime units work on processing the digital evidence used in computer crimes. A study was conducted analyzing these units. It suggested the specialized units operate more effectively than the non-specialized. This study also showed the lack of knowledge regarding standard procedures and the need for more training, funding, and personnel.
CHAPTER 1. INTRODUCTION

Technology is continuously growing throughout the world. With this expansion in technology, more and more people are taking advantage of the new technologies and using it to commit crimes (Brenner, 2004, 2011; Carnegie Mellon University, 2015). This led to the creation of computer forensics which involves the processing and analyzing of digital media to obtain evidence to be used in a court of law (Britz, 2009). Law enforcement agencies are having to examine many different types of digital media, but they are having a difficult time processing the amount of digital media being received in an effective and efficient manner (Clifford, 2011; Goodison, Davis, & Jackson, 2015). The Federal Bureau of Investigation as well as multiple states have set up cybercrime units to help process digital media (Jones & Valli, 2008; Schmitknecht, 2004). This study analyzed many different types of cybercrime units to determine whether or not they successfully process digital evidence and whether some units work better than others.

1.1 Scope

This study gathered data from multiple cybercrime units. The cybercrime units were classified into two groups: non-specialized and specialized. Information regarding the cybercrime unit as well as the digital evidence each unit has worked on was gathered and analyzed to determine how well the units were processing the digital evidence. This information included the number of personnel the unit had, the tools the unit members had, the number of cybercrime cases they received, the number of mobile phones processed, the number of computer hard drives processed, and so on. Information regarding why the unit was established, are officers being trained and/or certified, are resources being shared and are resources easier to
obtain was also gathered to determine if the structure of the units have an effect on processing digital media. Gathering this data allowed for an analysis on whether or not the units were successfully processing digital media and if the specialized cybercrime units were working more efficiently and effectively.

1.2 Significance

Over the centuries, crime has evolved with the existence of new technological resources (Holt, Bosslar, & Seigfried-Spellar, 2015). The capabilities that computers possess make it easier for users to gain access to a multitude of knowledge, to communicate almost instantaneously with someone on the other side of the world, and to create new technologies. While this alone seems like a positive advancement, there are still people who utilize this new technology to commit crimes. The crimes being committed include, but are not limited to, white-collar crimes, murder, terrorism, counterfeiting, drug dealing, and child pornography (Easttom, 2014). It is not only computer crimes that are the problem. Most crimes, regardless of being a computer crime, includes some sort of digital media (Clifford, 2011; Easttom, 2014). Processing digital media takes time and can easily double when multiple parties of a crime exist and each have their own digital device (Goodison et al., 2015).

Processing digital media takes time and can easily double when multiple parties of a crime exist and each have their own digital device (Goodison et al., 2015). Due to the vast amount of technology currently in existence, the vast amount of digital devices individuals have, and the rate at which technology changes, it is difficult for law enforcement agencies and investigators to keep up (Easttom, 2014). A study was conducted to determine if cybercrime units are successfully analyzing digital evidence and whether or not the specialized units are working more effectively than the non-specialized units. Determining if and why certain units are more effective may provide information to support the creation of similar units in other areas. Analyzing the cybercrime units may provide information that can definitively state these types of units are succeeding. This knowledge can also provide data that can help determine if existing units need to make changes to
better meet their goals and to process digital evidence more efficiently and more effectively.

1.3 Research Question

The goal of this study was to determine: Does having a specialized cybercrime unit increase efficiency and effectiveness in law enforcement agencies?

Efficiency was measured by the increase in number of cases and digital devices processed and effectiveness was measured by the reduction in the backlog of cases and the time taken to close a case.

1.4 Assumptions

The following assumptions were inherent to this study:

- The law enforcement units examined during this study have records of the cybercrimes they worked on.
- The law enforcement units presented legitimate records.
- The law enforcement units had data for at least one year after opening the unit.

1.5 Limitations

The limitations inherent to this study were as follows:

- The study was limited by the participation of each of the law enforcement units.
- The records the law enforcement units have may not all be the same across every unit examined.
• The units may not have numerical data prior to establishing the units.

1.6 Delimitations

The delimitations of this study included:

• Not all law enforcement units were analyzed.

1.7 Summary

Criminals are taking advantage of the expansion of technology and are making it difficult for law enforcement agencies to process all the digital evidence in an efficient and timely manner. Cybercrime units have been developed to help mitigate these circumstances. A study was completed to determine if specialized cybercrime units were operating more effectively and efficiently than the non-specialized cybercrime units.
CHAPTER 2. REVIEW OF RELEVANT LITERATURE

Digital forensics is a relatively new field compared to all the other sub-disciplines of forensic sciences (Holt et al., 2015). Consider the forensic science sub-discipline of fingerprints. Fingerprints were used by the Chinese in the 700s to determine the identity of documents (Inman & Rudin, 2000). Fingerprinting forensics has had over a thousand years to formalize and establish their forensic processes. The first computer, the ENIAC, was not even built until 1946 and was not fully operational until 1947 (Bergin, 2000). According to Clifford (2011), the history of computer crime started in the 1960s and was not recognized legally until the 1970s. Therefore, the field of digital forensics has only had about 45 years to evolve and establish their forensic processes.

Digital forensics evolved from computer forensics. Computer forensics refers to the processing and analysis of digital media to obtain evidence to present in a court of law (Britz, 2009). Digital forensics “refers to the analysis of digital evidence, which includes network forensics (Internet traffic), computer forensics, mobile-device forensics (e.g., cell phone), and malware forensics (e.g., viruses)” (Casey, 2011; Holt et al., 2015, p. 329). Therefore, computer forensics is a subset of digital forensics.

2.1 The Evolution and History of Digital Forensics

There have been three phases in this evolution. The first phase is considered to be the pre-forensics or the Ad Hoc phase. Computers were being developed but were originally owned by government agencies and universities (Holt et al., 2015). During this time, crimes involving computers comprised of stealing computer hardware (Holt et al., 2015). In the mid-1970s, personal computers became more
widespread and traditional crimes, such as embezzlement and fraud, were now being committed using this new technology (Clifford, 2011; Holt et al., 2015).

Computers were, and still are, used as an instrument to commit traditional crimes (Clifford, 2011), however, the tasks computers could complete and the time in which they could complete them led to new forms of criminal behavior (Clifford, 2011). The Internet was established in 1966 and its construction began in 1969 (Hafner & Lyon, 1998). The Internet was not widely used until the 1990s when the World Wide Web was established (Berghel, 1867). This new technology led to even more new forms of criminal behavior, such as hacking and malware. Not only are new crimes involving technology being created, but traditional crimes are being committed in new ways using technology. These traditional crimes include child pornography, fraud, and harassment (Casey, 2011; Holt et al., 2015). Laws in the 1970s were not written to accommodate computer related crimes, making it hard to prosecute computer criminal behavior (Clifford, 2011).

Senator Ribikoff proposed the first cybercrime legislation, the Federal Computer Systems Protection Act of 1977 (Clifford, 2011). Although this act was not passed, Senator Ribikoff provided awareness for the need of computer crime laws. Florida became the first state to implement a computer crime law, the Florida Computer Crimes Act of 1978 (Holt et al., 2015). During this phase, law enforcement agencies and corporations began to collect computer evidence and use computer forensic tools to obtain physical evidence (Charters, 2009; Holt et al., 2015). However, when these cases were brought to the courts, the methods and reliability of the forensic tools were questioned, especially since the original evidence was being analyzed and changes during this analysis was affecting the original evidence (Holt et al., 2015). The field, at this time, was not structuralized, and sufficient tools, processes, and procedures did not exist in the early 1980s (Charters, 2009; Holt et al., 2015).

The second phase, starting in the mid-1980s, is considered the structured phase (Charters, 2009). During this phase, computer crime laws and computer
forensic procedures were established (Holt et al., 2015). Laws were developed to condemn forms of hacking and wire fraud (Charters, 2009). Organizations began to create “appropriate use” policies and implementation and response methods (Charters, 2009). Courts also encouraged the need for forensic tools and procedures that could withstand courtroom challenges (Charters, 2009; Holt et al., 2015). Professional organizations began to form in response to the continuously changing technology. One such group was the Scientific Working Group on Digital Evidence (SWGDE) (Whitcomb, 2002). The first official definition for digital evidence was created during a SWGDE meeting: “any information of probative value that is stored or transmitted in a binary form” (Whitcomb, 2007, p. 7).

Towards the end of this phase is when the evolution from computer forensics to digital forensics occurred (Holt et al., 2015). The investigations began to include more forms of digital evidence, not just computers, such as mobile phones, cameras, and gaming consoles (e.g., PlayStation, Xbox) (Casey, 2011). These devices could be used for storage, communication, or as a means to search the Internet. Therefore, all of these devices may need to be analyzed as evidence during an investigation. These different devices and methods for analyzing them provided a need for more forensic tools.

The need for more forensic tools led to the third phase. The third phase, starting in the early 2000s, is known as the Enterprise phase or the Golden Age (Charters, 2009; Garfinkel, 2010). Forensic tools were developed and allowed to be used to analyze digital evidence (Holt et al., 2015). These tools help aid in the investigation process for analyzing digital media. The collection, preservation and analysis of digital media heavily rely on forensic tools (Garfinkel, 2010; Guo, Slay, & Beckett, 2009). The amount of storage a single device can contain has also increased and can be time consuming to complete a manual analysis, therefore, making the tools beneficial.

This third phase has led to the debate about whether digital forensics is a science (Gupta & Rogers, 2012). In 2008, the American Academy of Forensic
Science declared digital forensics as a scientific discipline (Olivier & Gruner, 2013). However, some do not view digital forensics as a science, but as technology. DeVore stated the difference between science and technology (DeVore, 1980). DeVore argued science involved exploring and understanding, while technology helps individuals to accomplish tasks. Gupta and Rogers (2012) argue digital forensics is both a science and technology, and is therefore, a technoscience. Investigative procedures depend on growing technology, however, digital forensic organizations use scientific methods to devise best practice methods within digital forensics. Many different methods for analyzing digital evidence have been created and are discussed more in the following section.

2.2 Cyberforensic Process Models

It was not until 1984 when the Federal Bureau of Investigations and other law enforcement agencies started to formalize the process for examining digital media for evidence (Noblett, Pollitt, & Presley, 2000). The digital forensics process, established thus far, “is to recover, analyze, and present computer-based material in such a way that it can be used as evidence in a court of law” (Easttom, 2014, p. 295). Four common steps exist in a digital forensic investigation: identification, acquisition, analysis, and presentation (Casey, 2011). The identification step involves identifying sources of digital evidence (e.g., computers, iPods, iPads, Kindles, USB drives, PlayStations, mobile phones) (ISO/IEC, 2012). The second step, acquisition, is to retrieve and preserve the digital evidence (ISO/IEC, 2012). The third step, analysis, involves the recovery and extraction of data (ISO/IEC, 2012). The fourth step, presentation, is to create a report containing information relevant to the investigation (ISO/IEC, 2012). There are several different models that have been developed that range in complexity and steps to gather, evaluate, and present digital evidence, however, an official standard has not yet been agreed upon for all agencies to use (Casey, 2011).
While four common steps exist, many models have been developed. These models aim at generalizing the digital forensic process for all digital media. Data from different digital media devices are retrieved differently (Easttom, 2014). Therefore, it is difficult to establish a single process of digital media evidence recovery for every scenario. Casey (2011) explains how the process models are either too detailed or too general and do not account for all scenarios. Casey (2011) also created a figure to display a few of the different process models and their steps (shown in Figure 2.1). It shows the steps within the processes side-by-side to show how the processes relate and how they differ.

Figure 2.1. Shows different digital forensic process models with both similar and distinct steps. Adapted from “Digital Evidence And Computer Crime: Forensic Science, Computers and the Internet (Third ed.) p. 189. Copyright 2011 by Elsevier Inc.”

In 1984, the Computer Forensic Investigative Process model was established and consisted of four steps: acquisition, identification, evaluation, and admission (Yusoff, Ismail, & Hassan, 2011). In 2001, the Digital Forensics Research Workshop suggested a six step model of: identification, preservation, collection, examination,
analysis, and presentation (Yusoff et al., 2011). Both of these models did not allow investigators to go to a previous step in that they are linear models. Therefore, the Abstract Digital Forensics Model (ADFM) was created in 2002 by Reith, Carr, and Gunsch. This model added three steps and also allowed for the investigator to continuously go back and forth between the examination and analysis phases (Yusoff et al., 2011). The nine steps within this model are: identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence (Baryamureeba & Tushabe, 2004).

The Integrated Digital Investigation Model (IDIP) was developed in 2003 by Carrier and Spafford. The IDIP model consisted of five sections of phases: the readiness phases, deployment phases, physical crime scene investigation phases, digital crime scene investigation phases, and the presentation phases (Baryamureeba & Tushabe, 2004). This model allows for interaction between the physical and digital crime scene investigation phases, however, the other phases are separate and are proceeded through linearly.

The Enhanced Digital Investigation Process Model (EIDIP) was developed in 2004 by Baryamureeba and Tushabe. This model consists of five main phases: readiness phases, deployment phases, traceback phases, dynamite phases, and review phases (Baryamureeba & Tushabe, 2004). This model allows for the investigation to iterate through the phases, meaning each phase can step back to the previous phase if needed.

The Hierarchical Objectives-Based Framework for Digital Investigations Process (HOBFDIP) was another model created in 2005 by Beebe and Clark. The HOBFDIP model consists of six steps: preparation, incident response, data collection, data analysis, presentation of findings, and incident closure (Beebe & Clark, 2005). The steps within this model are iterative, like the EIDIP model, however, each step breaks down into further steps.

Rogers (2007) criticized some of the models. He stated, the ADFM is too generic and not easily testable. The IDIP model is still too abstract and linear.
EIDIP model does not present new information and the sub-tasks are too confusing. The HOBFDIP is incomplete and tries to include everything making it too complex. Since these previous models still presented issues, Rogers came up with the Digital Crime Scene Analysis model in 2007. This model consisted of two main phases with a total of six sub-steps. The two phases consisted of corpus delicti and the lab (Rogers, 2007). Within the corpus delicti phase, the sub-tasks include evidence identification, evidence collection, and transportation. The lab phase consisted of the examination, analysis, and reporting of evidence (Rogers, 2007).

These models are just a few examples of all the different processes that have been developed to try to create a standard process for all law enforcement agencies to follow. However, it is difficult to create a model that will provide the necessary detail to process all different types of digital media and not be too complex.

2.3 A Growing Problem

Crimes involving computers are typically classified as one of three categories: crimes in which a computer is used as a tool in the crime, crimes in which the computer is the target of the crime, and crimes in which the computer is incidental (Brenner, 2004; Clifford, 2011; Goodman, 1997). Online fraud, theft of funds or information, embezzlement, stalking, forgery, homicide, and the creation and/or dissemination of child pornography are all examples of crimes in which the computer is used as a tool (Brenner, 2004; Clifford, 2011). Computers as a target in a crime include hacking, cracking, and distributed denial of service attacks (Brenner, 2004; Clifford, 2011). Crimes in which the computer is incidental to the crime includes crimes such as a drug dealer storing financial data of his buyers or the use of a computer to write a blackmail letter (Brenner, 2004; Clifford, 2011). In this case, computers are used as a “filing cabinet”. With the expansion of technology, more and more of these crimes are being committed.
As stated above, child pornography is a crime in which the computer is used as a tool. Law enforcement agencies focus highly on child pornography related crimes. National Center for Missing & Exploited Children (NCMEC) helps law enforcement with cases of missing and exploited children. In 2014, NCMEC received 1.1 million reports related to child exploitation, which increased significantly from 505,280 reports in 2013 (National Center for Missing & Exploited Children, 2014). In one year, the amount of reports NCMEC received almost doubled (National Center for Missing & Exploited Children, 2014). Child exploitation, child pornography, online enticement, child sex trafficking, and child molestation are the most prominent type of cybercrime cases (Clifford, 2011).

The Internet also makes it possible to easily commit so many other types of crimes as well, such as auto fraud, email scams, intimidation/extortion scams, real estate fraud, etc. (Internet Crime Complaint Center, 2014). The Internet Crime Complaint Center (IC3) was created in 2000 in order to handle these Internet crimes (Internet Crime Complaint Center, 2014). These Internet crimes do not include child exploitation crimes or crimes in which the computer is incidental. In 2013, the IC3 received 262,813 complaints and increased to 269,422 in 2014. The cost of these reported complaints was $800,492,073 (Internet Crime Complaint Center, 2014). The individual states loss is shown in Table 2.1. The number of complaints that the IC3 received from each individual state is shown in Table 2.2. Both tables rank the states from 1 to 51 because of the addition of District of Columbia as a separate entity. The data from these tables show the impact of a single complaint can cost thousands of dollars.
Table 2.1
*Dollar Loss Per State Reported to IC3*

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Dollar Loss</th>
<th>Rank</th>
<th>State</th>
<th>Dollar Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>$131,363,796</td>
<td>27</td>
<td>Oklahoma</td>
<td>$6,240,131</td>
</tr>
<tr>
<td>2</td>
<td>Florida</td>
<td>$52,544,107</td>
<td>28</td>
<td>Utah</td>
<td>$6,172,314</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>$50,116,593</td>
<td>29</td>
<td>Louisiana</td>
<td>$5,868,218</td>
</tr>
<tr>
<td>4</td>
<td>New York</td>
<td>$47,150,859</td>
<td>30</td>
<td>Alabama</td>
<td>$5,529,072</td>
</tr>
<tr>
<td>5</td>
<td>Arizona</td>
<td>$25,399,954</td>
<td>31</td>
<td>Kentucky</td>
<td>$5,342,414</td>
</tr>
<tr>
<td>6</td>
<td>Pennsylvania</td>
<td>$20,806,848</td>
<td>32</td>
<td>Kansas</td>
<td>$4,378,440</td>
</tr>
<tr>
<td>7</td>
<td>Illinois</td>
<td>$20,685,294</td>
<td>33</td>
<td>New Mexico</td>
<td>$4,177,508</td>
</tr>
<tr>
<td>8</td>
<td>New Jersey</td>
<td>$19,232,722</td>
<td>34</td>
<td>Arkansas</td>
<td>$3,972,610</td>
</tr>
<tr>
<td>9</td>
<td>Virginia</td>
<td>$16,571,859</td>
<td>35</td>
<td>Nebraska</td>
<td>$3,785,798</td>
</tr>
<tr>
<td>10</td>
<td>Georgia</td>
<td>$15,847,730</td>
<td>36</td>
<td>Idaho</td>
<td>$3,380,639</td>
</tr>
<tr>
<td>11</td>
<td>Washington</td>
<td>$14,780,493</td>
<td>37</td>
<td>New Hampshire</td>
<td>$3,025,825</td>
</tr>
<tr>
<td>12</td>
<td>North Carolina</td>
<td>$13,362,999</td>
<td>38</td>
<td>Iowa</td>
<td>$2,687,857</td>
</tr>
<tr>
<td>13</td>
<td>Michigan</td>
<td>$12,407,668</td>
<td>39</td>
<td>Mississippi</td>
<td>$2,580,678</td>
</tr>
<tr>
<td>14</td>
<td>Ohio</td>
<td>$12,345,292</td>
<td>40</td>
<td>Hawaii</td>
<td>$2,497,141</td>
</tr>
<tr>
<td>15</td>
<td>Massachusetts</td>
<td>$12,309,742</td>
<td>41</td>
<td>Delaware</td>
<td>$2,434,469</td>
</tr>
<tr>
<td>16</td>
<td>Nevada</td>
<td>$12,294,762</td>
<td>42</td>
<td>West Virginia</td>
<td>$2,330,137</td>
</tr>
<tr>
<td>17</td>
<td>Colorado</td>
<td>$11,487,488</td>
<td>43</td>
<td>District of Columbia</td>
<td>$1,551,758</td>
</tr>
<tr>
<td>18</td>
<td>Connecticut</td>
<td>$11,478,793</td>
<td>44</td>
<td>Rhode Island</td>
<td>$1,525,758</td>
</tr>
<tr>
<td>19</td>
<td>Minnesota</td>
<td>$9,441,547</td>
<td>45</td>
<td>North Dakota</td>
<td>$1,495,117</td>
</tr>
<tr>
<td>20</td>
<td>Wisconsin</td>
<td>$9,235,027</td>
<td>46</td>
<td>Alaska</td>
<td>$1,273,764</td>
</tr>
<tr>
<td>21</td>
<td>Oregon</td>
<td>$9,178,386</td>
<td>47</td>
<td>Wyoming</td>
<td>$1,236,741</td>
</tr>
<tr>
<td>22</td>
<td>South Carolina</td>
<td>$9,077,367</td>
<td>48</td>
<td>Vermont</td>
<td>$1,165,746</td>
</tr>
<tr>
<td>23</td>
<td>Maryland</td>
<td>$9,009,877</td>
<td>49</td>
<td>South Dakota</td>
<td>$1,023,368</td>
</tr>
<tr>
<td>24</td>
<td>Missouri</td>
<td>$7,156,094</td>
<td>50</td>
<td>Montana</td>
<td>$847,657</td>
</tr>
<tr>
<td>25</td>
<td>Tennessee</td>
<td>$6,453,385</td>
<td>51</td>
<td>Maine</td>
<td>$843,184</td>
</tr>
<tr>
<td>26</td>
<td>Indiana</td>
<td>$6,264,190</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note. IC3 = Internet Crime Complaint Center. Percentages are based on the total losses reported from all states and the District of Columbia. Adapted from 2014 Internet Crime Report by the Internet Crime Complaint Center, 2014, p. 21. Copyright 2014 by the Internet Crime Complaint Center.
Table 2.2

Number of Complaints Reported to IC3

<table>
<thead>
<tr>
<th>#</th>
<th>State</th>
<th>Number of Complaints</th>
<th>#</th>
<th>State</th>
<th>Number of Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>30,923</td>
<td>27</td>
<td>Oklahoma</td>
<td>2,027</td>
</tr>
<tr>
<td>2</td>
<td>Florida</td>
<td>18,637</td>
<td>28</td>
<td>Utah</td>
<td>1,825</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>16,954</td>
<td>29</td>
<td>Louisiana</td>
<td>2,382</td>
</tr>
<tr>
<td>4</td>
<td>New York</td>
<td>14,430</td>
<td>30</td>
<td>Alabama</td>
<td>3,202</td>
</tr>
<tr>
<td>5</td>
<td>Arizona</td>
<td>6,040</td>
<td>31</td>
<td>Kentucky</td>
<td>2,346</td>
</tr>
<tr>
<td>6</td>
<td>Pennsylvania</td>
<td>8,138</td>
<td>32</td>
<td>Kansas</td>
<td>1,688</td>
</tr>
<tr>
<td>7</td>
<td>Illinois</td>
<td>7,746</td>
<td>33</td>
<td>New Mexico</td>
<td>1,504</td>
</tr>
<tr>
<td>8</td>
<td>New Jersey</td>
<td>7,028</td>
<td>34</td>
<td>Arkansas</td>
<td>2,053</td>
</tr>
<tr>
<td>9</td>
<td>Virginia</td>
<td>7,112</td>
<td>35</td>
<td>Nebraska</td>
<td>880</td>
</tr>
<tr>
<td>10</td>
<td>Georgia</td>
<td>5,706</td>
<td>36</td>
<td>Idaho</td>
<td>1,057</td>
</tr>
<tr>
<td>11</td>
<td>Washington</td>
<td>6,388</td>
<td>37</td>
<td>New Hampshire</td>
<td>904</td>
</tr>
<tr>
<td>12</td>
<td>North Carolina</td>
<td>5,724</td>
<td>38</td>
<td>Iowa</td>
<td>1,454</td>
</tr>
<tr>
<td>13</td>
<td>Michigan</td>
<td>5,633</td>
<td>39</td>
<td>Mississippi</td>
<td>1,315</td>
</tr>
<tr>
<td>14</td>
<td>Ohio</td>
<td>6,114</td>
<td>40</td>
<td>Hawaii</td>
<td>1,020</td>
</tr>
<tr>
<td>15</td>
<td>Massachusetts</td>
<td>4,182</td>
<td>41</td>
<td>Delaware</td>
<td>802</td>
</tr>
<tr>
<td>16</td>
<td>Nevada</td>
<td>3,716</td>
<td>42</td>
<td>West Virginia</td>
<td>1,088</td>
</tr>
<tr>
<td>17</td>
<td>Colorado</td>
<td>4,953</td>
<td>43</td>
<td>District of Columbia</td>
<td>806</td>
</tr>
<tr>
<td>18</td>
<td>Connecticut</td>
<td>2,295</td>
<td>44</td>
<td>Rhode Island</td>
<td>582</td>
</tr>
<tr>
<td>19</td>
<td>Minnesota</td>
<td>2,876</td>
<td>45</td>
<td>North Dakota</td>
<td>360</td>
</tr>
<tr>
<td>20</td>
<td>Wisconsin</td>
<td>3,231</td>
<td>46</td>
<td>Alaska</td>
<td>2,379</td>
</tr>
<tr>
<td>21</td>
<td>Oregon</td>
<td>2,906</td>
<td>47</td>
<td>Wyoming</td>
<td>561</td>
</tr>
<tr>
<td>22</td>
<td>South Carolina</td>
<td>2,836</td>
<td>48</td>
<td>Vermont</td>
<td>382</td>
</tr>
<tr>
<td>23</td>
<td>Maryland</td>
<td>5,677</td>
<td>49</td>
<td>South Dakota</td>
<td>336</td>
</tr>
<tr>
<td>24</td>
<td>Missouri</td>
<td>3,487</td>
<td>50</td>
<td>Montana</td>
<td>691</td>
</tr>
<tr>
<td>25</td>
<td>Tennessee</td>
<td>3,909</td>
<td>51</td>
<td>Maine</td>
<td>726</td>
</tr>
<tr>
<td>26</td>
<td>Indiana</td>
<td>4,102</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

While child pornography and Internet crime cases are increasing and adding to the backlog of crimes law enforcement agencies face, crimes in which the computer is incidental (and technically not a computer crime) are also contributing to the backlog. The drug cases in which the drug dealer takes a picture of themselves with their drugs or has text messages stating they will buy or sell drugs on their mobile devices add to the backlog. Homicide crimes, stalking, robberies are all considered traditional crimes, however, even these crimes consist of some sort of digital evidence that needs processing for evidence (Clifford, 2011; Holt et al., 2015). Almost every crime involves at least one digital device (Clifford, 2011). The amount of digital evidence being received is difficult for law enforcement agencies to handle.

2.4 Challenges in Cyberforensics & Law Enforcement

One study showed that the issues, listed by priority, that the digital forensics community faces are: education\training\certification, technologies, encryption, data acquisition, tools, the legal justice system, evidence correlation, research, and funding (Rogers & Seigfried, 2004). This study was completed a decade later by Breitinger and Baggili (2015) and showed the priority of these issues have remained the same. According to Breitinger and Baggili (2015), the priority of issues were: education\training\certification, technologies, tools, evidence correlation, research, encryption, the legal justice system, and data acquisition and funding. Law enforcement officers are not trained in computer forensics, and therefore, they do not necessarily know the steps for the collection and analysis of digital media (Goodison et al., 2015). For example, when an officer finds a mobile device on the scene and needs it to be analyzed for evidence, the “best-practice” method of collection is to turn the device off or place the device in airplane mode (National Institute of Justice, 2008). Unless officers are informed of this process, they do not complete this process and it is possible that the device can be wiped of its data. Therefore, it may not be possible to retrieve any evidence from the device. While
there is training available for investigators, the funding to attend the training session or to receive certification is also lacking for many agencies (Holt et al., 2015; Rogers & Seigfried, 2004). There is also no established set of certifications or trainings that an investigator must complete.

Another problem that law enforcement agencies face is the different type of digital media devices and the different software installed on those devices. Digital media devices that law enforcement may need to analyze includes, but is not limited to, mobile devices, hard drives, tablets, cloud storage drives, flash drives, CD-ROMs, diskettes, cameras (Clifford, 2011). The evidence from each of these devices is retrieved differently. In order to recover data from a mobile device, law enforcement uses the UFED Cellebrite device that uses an automated process depending on the model of the phone and sometimes the network the mobile device is on (Cellebrite, 2015). When recovering data from hard drives, flash drives, or tablets, the software tools Forensic Toolkit (FTK) or Encase are used to make an image, a bit by bit copy, of the drive and to analyze the data found (AccessData, 2015; Guidance Software, 2015). FTK is used by more than 130,000 clients worldwide (AccessData, 2015). Although, these software tools can be used to automate the process of evidence retrieval, the location in which the data was stored is still different for each device. Law enforcement officers use the automated tools to make the process easier and faster, but they still need to verify that the tools work properly (Guo et al., 2009). For example, if the tool found an evidence item, the investigator needed to manually go to the location in which that item was found to verify that the evidence was there and that the tool found it correctly (Guo et al., 2009). The recovery and analysis of digital media is tedious.

The details and the knowledge that are required to complete a cyberforensics investigation can make it difficult to complete in a timely manner. Now that larger storage drives are readily available and relatively cheap, it is becoming more and more popular to find digital media devices that contain large amounts of data. A one terabyte drive, the equivalent of 60 stacks of computer paper as tall as the Eiffel
Tower, is not uncommon to find (Anon, 2010). Having to search this amount of data could take a long time (Goodison et al., 2015). Therefore, the automated tools are being used to help speed up that process. Even with these automated tools, it takes time. Due to the amount of time it takes law enforcement agencies to complete the cyberforensics investigations, the number of crimes committed, and the amount of digital evidence involved in those crimes, there is a backlog of digital media devices that need to be examined (Cohen, 2007). This backlog continues to grow. These are some of the many issues that the cyberforensics community faces.

2.5 Cyberforensics Laboratories

In order to help mitigate the issues the cyberforensics community faces, the FBI established the Regional Computer Forensics Laboratory (RCFL) model (Schmitknecht, 2004). This model would allow for a partnership and better collaboration between the FBI and other local law enforcement agencies to work together on cases providing more personnel and knowledge sharing between the agencies (Schmitknecht, 2004). According to the 2013 annual report, the FBI has 16 RCFL locations currently established (RCFL, 2013). These RCFLs are located in Chicago, Greater Houston, Heart of America, Intermountain West, Kentucky, Miami Valley, New Jersey, New Mexico, North Texas, Northwest, Orange County, Philadelphia, Rocky Mountain, San Diego, Silicon Valley, and Western New York.

In 2009, the RCFLs processed more than 6,000 examinations for 689 law enforcement agencies. The amount of digital evidence processed was 2,300 Terabytes (TB), which is about the contents of 230 academic libraries (RCFL, 2009). In 2013, the RCFLs helped 826 agencies and completed 7,273 digital examinations (RCFL, 2013). This consisted of 5,973 TB of data. Although, the RCFLs aided in many investigations, the RCFLs are not located in every state, and their primary focus are the federal cases and therefore, many local agencies are not getting the help they need.
Some states, in order to help solve this problem, established specialized cyberforensic units. However, research regarding the success of these units has yet to be conducted. The current study will assess these specialized units to determine if they are operating more efficiently and more effectively.

2.6 Summary

Digital forensics is a relatively new field compared to the other forensic science sub-disciplines. Since the digital forensics field is still new, computer forensic processing models and procedures have not yet been standardized. Therefore, in order to complete digital forensic investigations, it is best to follow the “best-practice” notion developed by the National Institute of Justice. There are many challenges law enforcement agencies encounter when processing digital media. The amount of digital devices needed to be analyzed is overwhelming. The procedures for processing digital evidence can be time consuming due to the amount of data digital media can store, not all law enforcement officers have the training to process digital media, and the different software installed on the digital media can change the procedure for processing the evidence. These challenges and the constant incoming flow of digital evidence is causing a backlog of evidence and makes it difficult for local law enforcement agencies to process the digital media in an effective manner. Law enforcement agencies have begun to address this problem by creating specialized cybercrime units to specifically process digital media.
CHAPTER 3. FRAMEWORK AND METHODOLOGY

The goal of this analysis was to determine whether the specialized cybercrime units were helping to process digital evidence more efficiently and effectively. It was expected the specialized units would perform at a better rate and quality than they were before the units were established.

In this study, a specialized cybercrime unit was a unit focused specifically on processing digital media and one that processed the digital evidence within their own unit. Non-specialized units were all other cyberforensic units. Also, the number of cases and digital evidence devices processed was used to measure efficiency. To measure effectiveness, a reduction in the backlog and time to close a case was required.

In order to complete this analysis, data was retrieved from different cybercrime units throughout the United States. These units were classified as a specialized or non-specialized unit. The units were then analyzed for their effectiveness and efficiency. A comparative analysis was completed using the specialized units verses the non-specialized units in order to determine if the specialized units were operating more efficiently and effectively. This chapter explains more about the data collection process and the analysis used to determine how well the cybercrime units were performing.

3.1 Hypothesis

Since specialized cybercrime units focus solely on digital evidence, the processing of digital media would be completed more efficiently and effectively.

The hypothesis for this study was the following:
H₀: The specialized cybercrime units process digital media more efficiently and effectively than the non-specialized units.

3.2 Unit & Sampling

The following section discusses the participants of the study, the data retrieval process, and the analysis.

3.2.1 Sample

Throughout the United States, law enforcement agencies have cybercrime units. A law enforcement agency from each state, including the District of Columbia, was contacted to determine if a cybercrime unit existed. In order to find these cybercrime units, Internet searches were completed to find digital forensic crime units associated with each state and a phone number associated with the units. A list of all these agencies was compiled. Then the phone number associated with the unit was called. Some of the phone numbers associated with the units were for forensic laboratories, attorney general’s offices, and others were the actual unit itself. Therefore, upon calling these phone numbers, some provided other contact information specifically for the cybercrime units. After contacting all of the states, 20 cybercrime units responded in favor of participating in the study. This was a response rate of about 39%.

3.2.2 Data Retrieval

Two surveys were conducted to determine if the cybercrime units were processing digital media more efficiently and effectively. Data collection included the use of phone interviews and an online survey. The phone interview acted as a qualitative analysis, and the online survey provided quantitative data. Two sets of surveys were created for the online questionnaire, one for specialized units and one
for non-specialized units. The only difference in the questions for the specialized units was to obtain additional numerical data from the unit before and after it was created.

Online research provided information to find the cybercrime units and their contact information, as stated in the previous section. Phone calls were made to find the personnel within the cybercrime units. Once the personnel from the cybercrime units were reached, they were asked if they would like to participate in the study. Contact information, such as direct phone numbers and emails, were obtained.

An email was sent to the member of the cybercrime unit (some of the members were the commander or director of the unit and others were not). This email stated the purpose of this study and what type of information was gathered to provide awareness and understanding of the study. Part of this email included the notification to keep the participants of the study confidential and to inform the participants the data retrieved would be anonymized and aggregated.

A time for the phone interview was then scheduled through phone calls and/or through emails.

The phone interview was conducted first to gain general knowledge about the unit, including when it was established, who was involved, and what counties the unit has served. Knowledge about why the unit was established, what was the purpose for opening the unit, what problems were occurring before the unit was created, whether the interviewee believes the unit has or has not been successful, and why it has or has not been successful was collected during this interview. This interview took approximately 30 minutes to complete.

The questions were developed prior to the interview. Some additional questions, however, were asked depending on the answers of the interviewees. Therefore, the interview was conducted in a semi-structured manner. The questions asked were open-ended questions. Some of the questions were based on previous research regarding the units to ensure the data retrieved was complete. These
interviews were also recorded for verification and validity of the study and of the notes taken during the interview.

The next part of the data collection process was quantitative and was more difficult because not all agencies keep the same type of statistics. The ideal collection of data consisted of the following data:

- number of mobile phones examined
- number of hard drives examined
- number of other digital media devices examined (eg. Kindle, iPad)
- number of leads reported to National Center for Missing and Exploited Children (NCMEC)
- number of cases sent to the Internet Crimes Complaint Center (IC3)
- number of computer crime cases
- average time spent on each type of case

Ideally, for specialized units, the units would have this collection data from before the specialized unit was created as well as after the unit created.

The quantitative data was retrieved via the online survey. This method of data collection allowed the survee to respond to these questions once the answers were obtained and to take their time answering them more than an on-the-spot interview would. Two online surveys were created using the Qualtrics tool. Qualtrics is a web-based survey software tool. Qualtrics allows the author of the survey to create the questions and to anonymize the respondents. The online survey can be distributed via email or through a link. Once the phone interview was completed, a link to the online survey was emailed to the cybercrime unit respondent. The link provided, was either the link to the non-specialized cybercrime unit survey or to the specialized cybercrime unit survey. The respondents were given a week to complete
the online survey. For those who did not complete the survey within five days, a reminder email was sent. This survey took approximately 15 minutes to finish.

Depending on information provided during the phone interview, the cybercrime unit was classified as specialized or non-specialized. Many of the units responded in favor of being specialized, only three did not. However, upon further internet research on the individual cybercrime units, it was found that some of the units, according to the definition in this study, were actually non-specialized. Therefore, some of the non-specialized units were asked the additional questions about before the unit was created that were not necessary.

Once this data was retrieved from both the phone interview as well as the online questionnaire, it was analyzed for all non-specialized and specialized units.

3.2.3 Comparative Analysis

A comparative analysis was completed using the data from the phone interviews and the online surveys. Analyzing the specialized crime units for the data before and after the unit was established was used to determine if the units were more efficient and effective as an individual specialized unit.

Next, an analysis was conducted to determine if the specialized units, in general, were working more efficiently and effectively than the non-specialized units.

In order to complete the comparative analysis for each individual specialized cybercrime unit, two main tasks were completed. First, the qualitative data retrieved from the phone interviews was analyzed to determine whether the interviewee believed the unit to be successful.

The second task for analyzing the data involved comparing the numerical data received from each of the specialized cybercrime units. The data from before the unit was established was compared to the data from after the unit was established. This showed whether the unit made an impact on the backlog of cases and if it was processing the digital evidence more efficiently and effectively.
statistical data suggests whether or not the units were processing more digital evidence and cases.

If the comparative analysis between the specialized and non-specialized units show the number of cases worked and the number of digital devices processed has increased, and the backlog and time to close a case has decreased, then the hypothesis will be correct in saying specialized cybercrime units were operating more efficiently and effectively than non-specialized units.

3.3 Summary

A study was completed to determine whether or not specialized cybercrime units were working more efficiently and effectively to process digital evidence. The data for this study was collected using two methods: a phone interview and an online survey. The data was then used in a comparative analysis to determine if the specialized cybercrime units were working more efficiently and effectively than non-specialized units.
CHAPTER 4. RESULTS

This chapter provides information from the study and the results from the comparative analysis. The number of cyberforensic units who agreed to participate in this study consisted of 20 units. All 20 units participated in the phone interview. However, only 16 out of the 20 units interviewed answered the online survey. Each of the units were classified as specialized or non-specialized based on two criteria. The first was whether or not the unit focused solely on cyberforensic cases and the second was whether or not the unit processed all of the digital media within their own unit. Upon classifying the units as specialized and non-specialized, the units that participated in the phone interview included 12 specialized and eight non-specialized. The online survey included eight specialized units and eight non-specialized units.

The participating units were found throughout the United States. The breakdown of the regions in which the survey participants were located is shown in Table 4.1. The regions are split into four categories: Pacific, Mountain, Central and Eastern.
Table 4.1
*Generalized Geographical Location of Participating Units*

<table>
<thead>
<tr>
<th>Variable</th>
<th>Unit Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Pacific (n = 6)</td>
</tr>
<tr>
<td>Participating States In Region</td>
<td>1 (16.7)</td>
</tr>
</tbody>
</table>

*Note: Values represent frequencies with percentages in parentheses.*

*Any percentage disparities due to rounding.*

The findings from both the phone interview as well as the online questionnaire are presented throughout this chapter.

4.1 Unit Descriptives

The phone interview was conducted to provide information about the unit. This part of the analysis was qualitative. The type of questions asked in this interview were developed to determine when and how the unit was set up. The questions also involved who the unit served and what type of cases the unit worked on.

4.1.1 Setup of the Unit

There were primarily four reasons for creating the units, regardless if the unit was specialized or non-specialized. The first reason was there was no one handling the digital evidence. Second, there was a continuous increase in digital evidence being seized. Third, they needed and wanted to share the resources. Finally, the last reason was the units were created to assist in crimes and provide
protection to the victims. Many of the units, 75% ($n = 15$), stated the primary reasons for creating the unit was because no one was processing the digital evidence and there was an increase in digital evidence.

Additional data regarding the agency primarily in charge of the cybercrime unit, the number of locations each unit contained, the year in which the unit was established, the number of counties the unit served, the number of personnel (including law enforcement officers and civilian personnel) involved in the unit, and whether or not the unit was a multi-agency unit is shown in Table 4.2. This data was meant to describe how the units were structured.
The units were typically overseen, or commanded, by a single person. The title of this person may be a Sergeant, Chief, Lieutenant, Captain, Special Agent, or Civilian Supervisor. While the commander may oversee the unit, not all of the

<table>
<thead>
<tr>
<th>Variable</th>
<th>Unit Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specialized (n = 12)</td>
</tr>
<tr>
<td>State Police</td>
<td>4 (33.3%)</td>
</tr>
<tr>
<td>Attorney General’s Office</td>
<td>1 (8.3%)</td>
</tr>
<tr>
<td>District Attorney’s Office</td>
<td>2 (16.7%)</td>
</tr>
<tr>
<td>Bureau of Investigation</td>
<td>2 (16.7%)</td>
</tr>
<tr>
<td>City Police</td>
<td>0 (0.0%)</td>
</tr>
<tr>
<td>Other</td>
<td>3 (25.0%)</td>
</tr>
<tr>
<td>Number of Locations Per Unit</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>8 (66.7%)</td>
</tr>
<tr>
<td>2</td>
<td>2 (16.7%)</td>
</tr>
<tr>
<td>3</td>
<td>1 (8.3%)</td>
</tr>
<tr>
<td>4 or more</td>
<td>1 (8.3%)</td>
</tr>
<tr>
<td>Year Established</td>
<td></td>
</tr>
<tr>
<td>before 2000</td>
<td>2 (16.7%)</td>
</tr>
<tr>
<td>2000-2005</td>
<td>5 (41.7%)</td>
</tr>
<tr>
<td>2006-2010</td>
<td>1 (8.3%)</td>
</tr>
<tr>
<td>2011-2015</td>
<td>4 (33.3%)</td>
</tr>
<tr>
<td>Number of Counties Served</td>
<td></td>
</tr>
<tr>
<td>1-30</td>
<td>6 (50.0%)</td>
</tr>
<tr>
<td>31-60</td>
<td>3 (12.0%)</td>
</tr>
<tr>
<td>61-90</td>
<td>2 (16.7%)</td>
</tr>
<tr>
<td>more than 90</td>
<td>1 (8.3%)</td>
</tr>
<tr>
<td>Number of Personnel</td>
<td></td>
</tr>
<tr>
<td>1-5</td>
<td>4 (33.3%)</td>
</tr>
<tr>
<td>6-10</td>
<td>6 (50.0%)</td>
</tr>
<tr>
<td>10 or more</td>
<td>2 (16.7%)</td>
</tr>
<tr>
<td>LEO Personnel</td>
<td></td>
</tr>
<tr>
<td>1-5</td>
<td>5 (41.7%)</td>
</tr>
<tr>
<td>6-10</td>
<td>5 (41.7%)</td>
</tr>
<tr>
<td>10 or more</td>
<td>2 (16.7%)</td>
</tr>
<tr>
<td>Civilian Personnel</td>
<td></td>
</tr>
<tr>
<td>1-5</td>
<td>11 (91.7%)</td>
</tr>
<tr>
<td>6-10</td>
<td>0 (0.0%)</td>
</tr>
<tr>
<td>10 or more</td>
<td>1 (8.3%)</td>
</tr>
<tr>
<td>Multi-agency Unit</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>8 (66.7%)</td>
</tr>
<tr>
<td>No</td>
<td>4 (33.3%)</td>
</tr>
</tbody>
</table>

*Note. Values represent frequencies with percentages in parentheses.

*Any percentage disparities due to rounding.

LEO = Law Enforcement Officer
commanders work within the cybercrime unit. One of the units, was not overseen by a single person, but by a board of individuals (some of which were in the unit and some were not).

4.2 Hypothesis Testing

The hypothesis for this study was specialized cybercrime units would process digital media more efficiently and effectively than the non-specialized units. To measure efficiency, there must be an increase in the number of cases and digital devices processed. Effectiveness was measured by the reduction in the backlog of cases and the time to close a case.

4.2.1 Efficiency Testing

One limitation stated in the methodology was whether or not the units kept data and whether or not they kept the same data. This limitation was seen in the data the units provided via the online survey regarding the number of cases processed before and after the unit was created. The data for the number of cases processed is shown in Table 4.3.
Table 4.3

Number of Cases Among the Units

<table>
<thead>
<tr>
<th>Variable</th>
<th>Specialized ( (n = 8) )</th>
<th>Non-specialized ( (n = 8) )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before</td>
<td>After</td>
</tr>
<tr>
<td>Total Value</td>
<td>Unknown</td>
<td>2481</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>4007</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>0 (2015)</td>
<td>44 (per year)</td>
</tr>
<tr>
<td></td>
<td>150</td>
<td>500 (per year)</td>
</tr>
<tr>
<td></td>
<td>500 (per year)</td>
<td>-</td>
</tr>
<tr>
<td>Unknown Given</td>
<td>3</td>
<td>800</td>
</tr>
<tr>
<td>(Yearly or Total)</td>
<td>60</td>
<td>17568</td>
</tr>
</tbody>
</table>

Note. Dash (-) = no answer given

As seen by the data in Table 4.3, the data is not uniform among the units. Some of the units did not know the number of cases processed before the unit was created. Only one specialized unit did not provide any data for the number of cases processed at all. The data also shows some of the values were given in cases per year and some in total cases throughout the years of the unit’s existence. During the phone interview, respondents stated there were a small number of digital cases, if any at all, being analyzed prior to creating the unit. This statement along with the numbers provided for after the unit was created show an increase in the number of cases. However, due to the data inconsistencies it is difficult to successfully analyze the number of cases processed.

Each case has a different amount of devices associated with it. The specific devices inquired about were computer hard drives, mobile phones, USB drives, kindles, ipads, and other tablets, gaming consoles, and other devices. Only one respondent added a specific device to the list. The added device was Micro SD cards. The data obtained from the units is displayed in Table 4.4. There were three units that did not provide any data regarding any of the devices. Out of the
remaining units, many of them did not keep information about the specific devices prior to establishing the unit. Out of the 13 units that did keep data, two (15%) of them had a decrease in the number of computer hard drives being processed. One of those two units was a newly established unit who had yet to see results regarding their unit.

Only one of the 13 units (8%) decreased in number of mobile phones analyzed. This decrease was also due to the newly created unit, who could not provide data for the time period after the unit’s creation.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Unit Category</th>
<th>Before</th>
<th>After</th>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer Hard Drives</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>154</td>
<td>0</td>
<td>15</td>
<td>650</td>
</tr>
<tr>
<td>Unknown</td>
<td>500</td>
<td>200</td>
<td>190</td>
<td>10</td>
<td>4000</td>
</tr>
<tr>
<td>Unknown</td>
<td>1000</td>
<td>20</td>
<td>300</td>
<td>Unknown</td>
<td>50</td>
</tr>
<tr>
<td>Unknown</td>
<td>60</td>
<td>29865</td>
<td>Unknown</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td><strong>Mobile Phones</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>212</td>
<td>0</td>
<td>5</td>
<td>129</td>
</tr>
<tr>
<td>Unknown</td>
<td>500</td>
<td>75</td>
<td>403</td>
<td>Unknown</td>
<td>1600</td>
</tr>
<tr>
<td>Unknown</td>
<td>1000</td>
<td>10</td>
<td>Unknown</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>800</td>
<td>0</td>
<td>Unknown</td>
<td>208</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>7000</td>
<td>Unknown</td>
<td>Unknown</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td><strong>USB Drives</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>27</td>
<td>0</td>
<td>800</td>
<td>351</td>
</tr>
<tr>
<td>Unknown</td>
<td>300</td>
<td>Unknown</td>
<td>Unknown</td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>20</td>
<td>100</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>Unknown</td>
<td>300</td>
<td>3</td>
<td>Unknown</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>2250</td>
<td>Unknown</td>
<td>Unknown</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td><strong>Kindles, iPads, and Other Tablets</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>3</td>
<td>81</td>
</tr>
<tr>
<td>Unknown</td>
<td>100</td>
<td>Unknown</td>
<td>Unknown</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>100</td>
<td>0</td>
<td>Unknown</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>200</td>
<td>0</td>
<td>Unknown</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>2750</td>
<td>Unknown</td>
<td>Unknown</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td><strong>Gaming Consoles</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>50</td>
<td>Unknown</td>
<td>Unknown</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>20</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>3</td>
<td>Unknown</td>
<td>Unknown</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td><strong>Other Devices</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>100</td>
<td>Unknown</td>
<td>Unknown</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>
| **Note.** The units responding with a total number of devices were labeled green. The units responding on a yearly basis were labeled red, and the units who did not specify yearly or total were labeled yellow.**
The two types of devices processed regularly among the units were computer hard drives and mobile devices. The number of USB drives processed after establishing the unit was the next largest category of devices processed. Regardless of whether or not the unit was specialized, individual units that provided data for both prior to the unit’s creation as well as after the unit’s creation showed there was an increase in number of devices being analyzed.

4.2.2 Effectiveness Testing

There were two criteria used to test effectiveness. These criteria included the reduction in backlog and a reduction in time to close a case.

4.2.2.1. Backlog

Upon analyzing digital evidence, the units reported a wide range of time for the backlogged cases. As shown in Table 4.5, about half of the units have a backlog of three months or less. However, due to the wide range of values it was difficult to compare the non-specialized units to the specialized units. The backlog for 66.7% \((n = 8)\) of the specialized units was three months or less. This value was more than 50% \((n = 4)\) of the non-specialized units.
A t test was conducted to assess the mean difference between specialized and non-specialized units on the backlog provided after the units were created. The months reported were used in this analysis and not the combined categories provided in Table 4.5. The t test shows the differences between two means. The t test showed there was no significant difference between the backlog of the specialized (\(M = 3.2, SD = 3.4\)) and non-specialized units (\(M = 5.9, SD = 6.4\)), \(t(16) = -1.14, p = .27\).

While the descriptive statistics do not show a significant difference among the non-specialized and the specialized units for the reduction in backlog, the values provided by the units suggest there was a difference. The backlog for 66.7% (\(n = 8\)) of the specialized units had a backlog of three months or less. For the non-specialized units, 50% (\(n = 4\)) of them had a backlog of three months or less.
4.2.2.2. Time to Close Cases

The time spent on a case was different between the units. The data from before and after the unit was created is shown in Table 4.6. The data from the units that provided an answer to this question shows the majority of the time taken to close a case was less than six months, regardless if the unit was specialized or non-specialized.

Table 4.6

<table>
<thead>
<tr>
<th>Time Spent On A Case</th>
<th>Unit Category</th>
<th>Specialized (n = 8)</th>
<th>Non-specialized (n = 8)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before</td>
<td>After</td>
<td>Before</td>
</tr>
<tr>
<td>Less than a week</td>
<td>2 (25.0)</td>
<td>2 (25.0)</td>
<td>2 (25.0)</td>
</tr>
<tr>
<td>Less than a month</td>
<td>0 (0.0)</td>
<td>2 (25.0)</td>
<td>0 (0.0)</td>
</tr>
<tr>
<td>Less than six months</td>
<td>3 (37.5)</td>
<td>1 (12.5)</td>
<td>1 (12.5)</td>
</tr>
<tr>
<td>Less than a year</td>
<td>1 (12.5)</td>
<td>0 (0.0)</td>
<td>0 (0.0)</td>
</tr>
<tr>
<td>More than a year</td>
<td>0 (0.0)</td>
<td>0 (0.0)</td>
<td>0 (0.0)</td>
</tr>
<tr>
<td>Did not answer</td>
<td>2 (25.0)</td>
<td>3 (37.5)</td>
<td>5 (62.5)</td>
</tr>
</tbody>
</table>

Note. Values represent frequencies with percentages in parentheses.
*Any percentage disparities due to rounding.

Another t test was completed to test the mean difference between specialized units and the non-specialized units based on the time taken to close a case. The t-test stated there was no significant difference for the time taken to close a case between the specialized ($M = 1.8, SD = 0.8$) and non-specialized units ($M = 2.0, SD = 0.5$), $t(11) = -.53$, $p = .61$. On average, both units reported approximately less than one month to close a case.

4.3 Exploratory Analysis

Due to the anticipation of a lack of records kept by the units, exploratory analyses were conducted beyond the hypothesis to better understand the specialized
and non-specialized units. The next section discusses the findings from the exploratory analyses.

4.3.1 Unit Funding

The funding of these units is an important factor to consider. In order to establish and maintain the units, some of the units received funding from different agencies as shown in Table 4.7. The data shows the units were created with limited funding. However, in order to maintain the unit funding was more likely obtained. The units that received funding upon creating the unit received the funding from the Department of Justice (DOJ), the National Institute of Justice (NIJ), a state funded grant, or a federal funded grant. In order to maintain the unit, the majority of the funding came from the DOJ using the Internet Crimes Against Children (ICAC) distribution money, however, other grants were received through the NIJ, the United States Secret Service, the Federal Bureau of Investigation, and other state funded organizations. The units that were considered multi-agency units that paired with a University had more opportunities to receive grant funding, primarily from NIJ.

Table 4.7

<table>
<thead>
<tr>
<th>Variable</th>
<th>Unit Category</th>
<th>Specialized (n = 12)</th>
<th>Non-specialized (n = 8)</th>
<th>Total (n = 20)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funding</td>
<td>Yes</td>
<td>3 (25.0)</td>
<td>4 (50.0)</td>
<td>7 (35.0)</td>
</tr>
<tr>
<td>Upon</td>
<td>No</td>
<td>8 (66.7)</td>
<td>4 (50.0)</td>
<td>12 (60.0)</td>
</tr>
<tr>
<td>Creation</td>
<td>Unknown</td>
<td>1 (8.3)</td>
<td>0 (0.0)</td>
<td>1 (5.0)</td>
</tr>
</tbody>
</table>

Note: Values represent frequencies with percentages in parentheses.

*Any percentage disparities due to rounding.
4.3.2 Unit Certifications and Tools

There are many different certifications available for cyberforensic laboratories. A specialized certification for crime laboratories is the American Society of Crime Lab Directors (ASCLD) certification. Many of the units, 19 out of 20 units (95%) responded they were not ASCLD certified. The single unit, a non-specialized unit, that responded they were ASCLD certified, stated it was their parent laboratory that was ASCLD certified. There was one (5%) unit planning to get ASCLD certified within the next five years. Another two (10%) units stated they were inquiring about the ASCLD certification. There were seven units (35%) that looked into getting the certification, but decided against it. They stated the certification was too costly or the ASCLD requirements do not make sense in the digital world.

The personnel within the units have different certifications. The certifications among the units included the International Association of Computer Investigative Specialists (IACIS) certification, the Seized Computer Evidence Recovery Specialist (SCERS), the FBI Computer Analysis and Response Team (CART) certification, Peace Officer certification, or the Global Information Assurance Certification (GIAC). These certifications are used to train individuals about cyberforensic investigations. Vendor specific certifications among the units included AccessData Certified Examiner (ACE), EnCase Certified Examiner (EnCE), Cellebrite, A+, Security+, Network+, and many more. These vendor certifications are for specific tools or for specific cyberforensic topics. The details of the certifications the specialized units had verses the non-specialized units are shown in Table 4.8.
Some of the vendor specific certifications provide information about some of the tools the units used. While some tools have certifications available not all of them do. The units provided many different tools used during their investigations. The different tools used range widely. However, there were five tools used by most of the units. These tools, in order of most used, were AccessData’s FTK and Cellebrite both being used in 90% \((n = 18)\) of the units. Internet Evidence Finder was used by 75% \((n = 15)\) of the units. Encase was used by 60% \((n = 12)\) of the units. Finally, X-Ways Forensics was used by 50% \((n = 10)\) of the units. Katana Forensics Lantern, BlackBag’s BlackLight, Oxygen Forensics and Susteen were among some of the additional tools used.
Although some of the unit personnel may have been specialized in certain areas, for the most part, specific roles for processing digital evidence were not assigned to specific people. The personnel processed all types of digital evidence and not just the digital evidence for their specialized areas. Only 10% \((n = 2)\) of the units needed to send their evidence to outside agencies, such as the RCFL, for processing (this did not include the units that did not have advanced forensic techniques such as JTAG and need to send the digital evidence out for this type of analysis).

When conducting an investigation and processing the digital evidence, 95% \((n = 19)\) of the units follow some set of standard operating procedures. Many of the units could not provide a specific set of standard procedures, but stated they follow the “best-practice” standards among the digital forensics community.

4.3.3 Unit Cases

There are many different aspects of a digital forensic case. The case may be classified as federal, state, or local. There are also many different types of cases, such as child pornography related cases, drug related cases, or homicide related cases. Each of these cases may require a different type of digital forensic analysis, such as computer forensics, mobile forensics, or network forensics. Data was obtained about each of these items from the units.

4.3.3.1. Case Classification

The classification of cases (federal, state, or local) in which the units work differs among the units. Figure 4.1 shows the differences in percentage of cases worked by specialized and non-specialized units. Both the specialized and non-specialized units work on state and local cases. The federal cases are primarily worked on by specialized units.
Figure 4.1. Shows the number of units working on federal, state and local cases.

Using percentages obtained from the online questionnaire, a more detailed analysis of the time spent on federal, state, and local cases was obtained. Table 4.9 shows the percentage of time spent on federal, state and local cases among the 16 units who responded to the online questionnaire.
### Table 4.9

**Number of Units Working on Federal, State and Local Cases.**

<table>
<thead>
<tr>
<th>Unit Classification</th>
<th>PoT Units Work</th>
<th>Federal</th>
<th>State</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-20</td>
<td>7 (87.5)</td>
<td>3 (37.5)</td>
<td>3 (37.5)</td>
<td></td>
</tr>
<tr>
<td>21-40</td>
<td>1 (12.5)</td>
<td>1 (12.5)</td>
<td>1 (12.5)</td>
<td></td>
</tr>
<tr>
<td>Specialized (n = 8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41-60</td>
<td>-</td>
<td>2 (25.0)</td>
<td>1 (12.5)</td>
<td></td>
</tr>
<tr>
<td>61-80</td>
<td>-</td>
<td>2 (25.0)</td>
<td>1 (12.5)</td>
<td></td>
</tr>
<tr>
<td>81-100</td>
<td>-</td>
<td>0 (0.0)</td>
<td>2 (25.0)</td>
<td></td>
</tr>
<tr>
<td>0-20</td>
<td>7 (87.5)</td>
<td>3 (37.5)</td>
<td>3 (25.0)</td>
<td></td>
</tr>
<tr>
<td>21-40</td>
<td>0 (0.0)</td>
<td>3 (37.5)</td>
<td>0 (0.0)</td>
<td></td>
</tr>
<tr>
<td>Non-Specialized (n = 8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41-60</td>
<td>-</td>
<td>1 (12.5)</td>
<td>3 (37.5)</td>
<td></td>
</tr>
<tr>
<td>61-80</td>
<td>1 (12.5)</td>
<td>0 (0.0)</td>
<td>0 (0.0)</td>
<td></td>
</tr>
<tr>
<td>81-100</td>
<td>-</td>
<td>1 (12.5)</td>
<td>3 (37.5)</td>
<td></td>
</tr>
</tbody>
</table>

*Note.* Values represent frequencies with percentages in parentheses.

*Any percentage disparities due to rounding.

PoT = Percentage of time

#### 4.3.3.2. Types of Crime

The type of crime in which the units work also differed. A small portion of units, two (10%), were limited to felony crimes only. One of these felony-focused units was specialized and the other was non-specialized. The majority of the units worked on all types of crimes, with some focusing on crimes against children. The number of units who worked on the different types of crimes are shown in Table 4.10.
Table 4.10

Number of Units Working on Specific Types of Crimes.

<table>
<thead>
<tr>
<th>Type of Crime</th>
<th>Specialized (n = 12)</th>
<th>Non-Specialized (n = 8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Types of Crime</td>
<td>5 (41.7)</td>
<td>2 (25.0)</td>
</tr>
<tr>
<td>Focus on CAC, but Work All</td>
<td>6 (50.0)</td>
<td>3 (37.5)</td>
</tr>
<tr>
<td>Only CAC</td>
<td>0 (0.0)</td>
<td>2 (25.0)</td>
</tr>
<tr>
<td>Only Felonies</td>
<td>1 (8.3)</td>
<td>1 (12.5)</td>
</tr>
</tbody>
</table>

*Note. Values represent frequencies with percentages in parentheses.*

*Any percentage disparities due to rounding.*

CAC = Crimes Against Children

The types of cases that involve digital evidence among the units include, but are not limited to, child pornography cases, drug cases, homicide cases, robbery cases, sexual assault cases, and fraud cases. The percentage of time spent on child pornography cases involving digital evidence is high compared to the other crimes regardless if the units are specialized or non-specialized. The average percentage of time spent on each type of case involving digital evidence are shown in Table 4.11. Only two (12.5%) of the units did not spend the majority of the time on child pornography cases. One of these two units did not work on any child pornography cases. They sent their cases to the RCFL.
4.3.3.3. Types of Digital Forensics

When processing digital forensic cases, the online questionnaire assessed the type of digital forensic investigations conducted by the unit (e.g., computer forensics, mobile forensics, network forensics, malware forensics, video forensics, social media forensics, vehicle forensics, audio forensics, and camera forensics). According to the data shown in Table 4.12, all 16 of the units work on both computer forensics and mobile forensics. The data also shows that non-specialized units conduct malware forensics more frequently than specialized units.

The most prevalent type of digital forensics completed by all of the units were computer forensics and mobile forensics. Computer forensics was the most prevalent type of digital forensics among 31% \((n = 5)\) of the units. Mobile forensics was the most prevalent among 69% \((n = 11)\) of the units.
Between all 16 units, the majority of their time was spent as digital forensic examiners. Only two (12.5%) units reported spending more time as an investigator verses as a digital forensic examiner. The units spent at least 75% of their time as a digital forensic examiner 87.5% \((n = 14)\) of the time.

### 4.3.4 Organizations Aiding in Digital Forensic Cases

Two widely known organizations that aid law enforcement with cybercrime cases are NCMEC and IC3. NCMEC is an organization that helps with child exploitation cases. Only nine of the 16 units (56%) responded with data about the NCMEC leads obtained before and after the units were created. All of the units that responded had an increase in number of NCMEC leads. The data for NCMEC leads are shown in Table 4.13.
Table 4.13
Number of NCMEC Leads and IC3 Reports

<table>
<thead>
<tr>
<th>Variable</th>
<th>Specialized ($n = 8$)</th>
<th>Non-specialized ($n = 8$)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before</td>
<td>After</td>
</tr>
<tr>
<td>NCMEC</td>
<td>3</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>23000</td>
</tr>
<tr>
<td>IC3</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>70</td>
<td>800</td>
</tr>
</tbody>
</table>

Note. For the NCMEC leads, only five specialized units and four for the non-specialized units reported statistics. For the IC3 reports, only three specialized units and one non-specialized unit reported statistics. NCMEC = National Center for Missing and Exploited Children, IC3 = Internet Crime Complaint Center

The IC3 organization helps in crimes related to fraud and other internet related crimes (excluding child exploitation cases). A smaller number of units report incidents to the IC3. Only four of the 16 units (25%) responded with data for IC3 reports. One of the four units (25%) had a reduction in the number of IC3 reports from before and after the unit was created. Another unit only had one additional report to the IC3 organization from before and after the unit was created. The data for the IC3 reports is shown in Table 4.13.

4.4 Unit Recommendation

During the phone interview, the interviewee was asked if they believed the unit was successful, 75% ($n = 15$) of the respondents stated the unit was successful. They stated they believed the unit was doing well in processing the digital evidence
and the court success rates were good. Twenty-five percent of the units responded the unit had not succeeded mostly due to the need for more personnel. One unit, stated they were not successful yet because the unit was a fairly new unit and had not had the opportunity to see success or failure yet. The comparison between the specialized and non-specialized units is shown in Table 4.14 and shows the success rate to be the same among both types of units.

<table>
<thead>
<tr>
<th></th>
<th>Specialized ((n = 12))</th>
<th>Non-Specialized ((n = 8))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>9 (75.0)</td>
<td>6 (75.0)</td>
</tr>
<tr>
<td>No</td>
<td>3 (25.0)</td>
<td>2 (25.0)</td>
</tr>
</tbody>
</table>

*Note.* Values represent frequencies with percentages in parentheses.

*Any percentage disparities due to rounding.*

The interviewee was also asked whether or not the creation of a similar unit is recommended. There were two responses: yes, absolutely and it depends. None of the interviewees said no they would not recommend the unit. There were 13 (65%) units that stated yes, absolutely. Seven (35%) of the units responded it depends. Upon responding with yes, the reasons provided were a similar unit could help with the backlog, smaller agencies could use the resources, and technology and digital evidence is continuously increasing. Those that responded it depends, stated it is incredibly expensive to operate this type of unit, it depends on the types of problems being faced, and it depends if there is a need for it.
Table 4.15
*Unit Creation Recommendation*

<table>
<thead>
<tr>
<th>Recommend</th>
<th>Specialized (n = 12)</th>
<th>Non-Specialized (n = 8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>8 (66.7)</td>
<td>5 (62.5)</td>
</tr>
<tr>
<td>No</td>
<td>4 (33.3)</td>
<td>3 (37.5)</td>
</tr>
</tbody>
</table>

*Note.* Values represent frequencies with percentages in parentheses.

*Any percentage disparities due to rounding.*

The breakdown between the specialized and non-specialized units is shown in Table 4.15. Both the specialized and non-specialized have similar rates for recommendation as well.

**4.5 Summary**

The data retrieved from the phone interviews as well as the online questionnaires provided many insights about the units. However, due to the limitations of the data for the number of cases and digital devices processed it cannot be determined if the specialized units were operating more efficiently than the non-specialized units. The limitations of the numbers for the backlog also make it difficult to show whether or not the specialized units were operating more effectively than the non-specialized units. Descriptive statistics for the backlog and the time taken to close a case do show, however, there is no significant difference between the two groups.
CHAPTER 5. DISCUSSION

This study analyzed data collected from different cybercrime units from around the United States. The goal of this study was to show whether or not specialized cybercrime units process digital media more efficiently and effectively than the non-specialized cybercrime units. In this study, efficiency was measured by an increase in the number of cases and digital evidence items processed. Effectiveness was measured by the reduction in backlog and time taken to close a case. This study consisted of two surveys: a phone interview and an online questionnaire.

There were 20 cybercrime units that participated in the phone interview and 16 cybercrime units in the online questionnaire. Therefore, the study had an unbalanced design. The purpose of the phone interview was to gather qualitative data about the unit. This qualitative data included information about the unit’s structure, its creation, grant funding, the certifications and tools used by the unit, and the unit’s backlog. The online questionnaire was used to obtain the quantitative data. This data included information about the cases, such as the type of cases, the digital forensics involved, the number of cases, the number of devices, and the time taken to close a case. The data each of the units kept, limited the findings of this study. Therefore, there is not enough data to show a statistical difference between the effectiveness and efficiency of the specialized and non-specialized units.

The results showed, the specialized units have a larger number of locations and have more personnel (especially law enforcement officers) within the units. The number of personnel within the units was a concern that many of the units had. The lack of personnel was the primary reason for those that stated they were not successful.
The specialized units were more likely to be a multi-agency unit. The multi-agency units had two advantages. First, the units found it more cost effective to share the resources they had among all the agencies involved in the unit. Second, the units working with universities had more opportunities to obtain grant funding.

Funding was also another large concern for the units. While many of the units received funding for their work with ICAC cases, these units are expensive to open and operate. Therefore, applying for grant funding may be beneficial to many of these units. In order to apply for these grants, many units need to have and certify that they follow a standard set of procedures.

The standard procedures for processing digital media among the units differed greatly. The units stated they followed standard procedures, however, many of them could not name a particular set of procedures. This problem coincides with the argument made by previous literature that the digital forensic community has yet to develop a standard set of procedures to encompass all digital investigations (Casey, 2011; Rogers, 2007). The lack of knowledge regarding what set of standard procedures the units follow may be used in court by defense attorneys, especially the unit that stated no standard procedures were followed. It also shows the lack of agreed upon standards within the digital forensic community.

The certifications the unit personnel possessed differed among the specialized and non-specialized units. The specialized units were more likely to have been IACIS certified, while the non-specialized units were certified through many different programs other than IACIS. Previous studies showed certifications to be a leading issue within the digital forensic community (Breitinger & Baggili, 2015; Rogers & Seigfried, 2004). IACIS is an international cyberforensic training program and would be beneficial to obtain.

According to the structure of the units, it is beneficial to create a specialized unit if the unit needs more personnel, more funding opportunities, and the IACIS certification.
This study also showed a wide range of tools used by each of the units. There were three tools in which most of the units used, AccessData’s FTK, Cellebrite, and Internet Evidence Finder. While there were three main tools all of the units used, there were many tools in which only a couple units used. The wide range of tools supports previous research that stated tools were an issue among the cyberforensic community (Breitinger & Baggili, 2015; Rogers & Seigfried, 2004). Besides the three main tools, the community does not have a standard set of tools to conduct investigations.

For the cases processed within the units, the classification, types of crime, and types of digital forensics were similar. The two main differences between the units were specialized units were more likely to work on federal cases and non-specialized units were more likely to conduct malware forensics. Therefore, the cases processed among the specialized or non-specialized units should not be used to determine if a specialized unit is more beneficial.

Upon analyzing the data used to support or refute the hypothesis, the limitations of this study were reached. The two main limitations of this study were the units may not keep records of the digital evidence processed and the units may not keep the same records of digital media analyzed. Many of the units did not keep records from before the unit was created. Therefore, the data from before and after the unit was created could not be compared. The data provided by the units was also different. Some of the units provided yearly data verses the total amount of data. This problem occurred when analyzing the data for the number of cases and digital devices processed. Therefore, it was difficult to analyze the data to show whether or not the specialized units were more efficient.

Looking at the data from the units, without calculating descriptive statistics, does show an increase in the number of cases regardless if the unit was specialized or non-specialized. This is consistent with analyzing more cases, and it may also be consistent with the increase in crimes involving digital evidence and therefore, more cases being analyzed.
The data reported for the backlog among the units was not kept by many of the units prior to their creation. However, descriptive statistics were calculated to provide information about the backlog after the unit was created and the time taken to close cases. The descriptive data showed there was not a significant difference among the means between the specialized and non-specialized units. However, the data provided by the units did suggest that more specialized units have a lower backlog. If a larger sample size was analyzed, it is likely there will be a statistical difference in the backlog among the specialized and non-specialized units. Therefore, with a larger sample size, it is likely the specialized units operate more effectively than the non-specialized units.

While the data was difficult to analyze according to the definitions provided in this study of efficiency and effectiveness, insights did provide support for creating the specialized units. The structure of the specialized units showed, in general, the number of cases and digital devices processed has increased, and in general, the backlog of cases for specialized units was lower than non-specialized units.

5.1 Recommendations

The data from this study provided many interesting insights, however, it may be better to analyze the units on a year to year basis rather than before the unit was created and after the unit was created. Another aspect of this study that can be improved upon is the number of units analyzed. While a reasonable amount of units responded to this survey, the variables were changing quite a lot with a single unit answering differently than others. This in part was due to the inconsistent records kept by the units as well as the lack of answers from some of the units. Therefore, while it would be difficult for the units to determine all of the data from previous years, it is recommended that a standard set of records be kept by all units.

Upon contacting the Regional Computer Forensic Laboratory (RCFL), it was found that the records they keep per year are:
• Number of cases
  - From which agency did the case come from
  - Is the case federal, state, or local
• What crime types involve digital media (e.g. homicide, robbery, drug)
• Number of hard drives
• Number of cell phones
• Number of flash drives
• Number of digital cameras
• Total number of Gigabytes processed throughout the year
• Number of devices running Windows, Linux, Unix, or Macintosh

While the RCFL did not mention keeping the following records, it is recommended that the additional items be recorded per year:

• Number of kindles, iPads, and other tablets
• Number of gaming consoles
• Backlog in number of months
• Average time it takes to close a case
• Number of personnel working on crimes involving digital media
• Operating budget

Having a standardized set of data from all the cybercrime units will help to provide more quality data. These records can also be used to obtain grants. Many grants, such as NIJ, ask for these types of records to fulfill their evidence-based policy.
5.2 Summary

This study presents many different findings for both non-specialized and specialized units. Although the records among the units are not consistent, it was still possible to determine that the specialized units in general were operating more effectively. A larger sample size may provide more conclusive findings. Many improvements can be made upon this study and can be conducted in the future, however, this is a good basis point for analyzing all cybercrime units.

The questionnaire developed can provide a basis point for future research. The questions in which the interviewees did not necessarily understand can be worded differently. The questions in which surprising answers were found can also be worded differently and/or expanded upon to obtain a better understanding of these answers.

More future work could include the analysis of units in other countries. This study focused on units within the United States and while there are some similar organizations that operate similarly there are some in which their structure is different. The types of cases being worked on in Europe are more complicated than the cases in the US (Europol, 2016).

The recommendations for a standard set of records among digital forensic practitioners can be beneficial to the practitioners as well as the researchers. The practitioners can use the records to write effective grants to apply for more funding and can also show what the unit is doing well in and what they need to improve.
LIST OF REFERENCES
LIST OF REFERENCES


Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. DFRWS.


Bergin, T. J. (2000). 50 years of army computing from ENIAC to MSRC.


APPENDICES
CHAPTER A. IRB APPROVAL REQUEST
INSTRUCTIONS

Failure to follow these instructions may result in the submission being returned to the principal investigator.

1. Use this form to request an exemption under Title 45 CFR §46.101(b)(2) or (3).
2. Use lay language and spell out acronyms. Do not cut and paste from or refer to grant or abstract.
3. Study activities may not be implemented until the investigator receives final written IRB notification the exemption has been granted.
4. In order to qualify for either of these exemptions, the study must fall into one of the following categories. Additionally you may wish to consult the decision chart for these categories.
5. Research involving PRISONERS or other incarcerated individuals (or their existing data and/or specimens) do not qualify for exemption.

Category 2 involves ONLY the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless:
* information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and
* any disclosure of the human subjects’ responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects’ financial standing, employability, or reputation.

Category 3 involves the use of ONLY the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior that is not exempt under category 2, if:
* the human subjects are elected or appointed public officials or candidates for public office; or
* federal statute(s) require(s) without exception that the confidentiality of the personally identifiable information will be maintained throughout the research and thereafter.

* PRISONER – means any individual involuntarily confined or detained in a penal institution. The term is intended to encompass individuals sentenced to such an institution under a criminal or civil statute. Individuals detained in other facilities by virtue of statutes or commitment procedures which provide alternatives to criminal prosecution or incarceration in a penal institution, and individuals detained pending arraignment, trial, or sentencing (45 CFR 46.101(c)).

INVESTIGATOR INFORMATION

HAVE QUESTIONS about this section?
Principal Investigator Eligibility policy
Your Role and Education Requirements guidance

1. Principal Investigator contact information:

<table>
<thead>
<tr>
<th>Name and Title</th>
<th>Department</th>
<th>Campus Address</th>
<th>Phone</th>
<th>Email</th>
<th>CITI Training Complete?</th>
<th>Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Katheya Seigfried-Spelar</td>
<td>CNIT</td>
<td>499 N Grant St</td>
<td>765-694-2430</td>
<td><a href="mailto:kspeller@purdue.edu">kspeller@purdue.edu</a></td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

Example 2-3 v. 113
2. Co-Investigators and/or Key Personnel contact information:

<table>
<thead>
<tr>
<th>Name and Title</th>
<th>Department/ Institution</th>
<th>Phone</th>
<th>Email</th>
<th>Directly Interacting with Subjects? Y/N</th>
<th>CITI Training Complete? Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaitlyn Gurule</td>
<td>CNIT</td>
<td>505-221-4650</td>
<td><a href="mailto:kgrule@purdue.edu">kgrule@purdue.edu</a></td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

3. Consultant(s) contact information:

<table>
<thead>
<tr>
<th>Name and Title</th>
<th>University/ Institution</th>
<th>Phone</th>
<th>Email</th>
<th>Directly Interacting with Subjects or Assessing Identifiable Information? Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CONFLICT OF INTEREST

4. Do the investigators or personnel have a significant financial interest in this study?
   ☑ NO - If no, skip to question 5.
   ☐ YES - If yes, proceed to question 5.

5. Has a Significant Financial Interest Disclosure Form been filed?
   ☑ NO - If no, refer to Financial Conflict of Interest: Policy and Procedures.
   ☐ YES - If yes, proceed to question 6 below.

6. Do the investigators or personnel have any other known conflict of interest in this study?
   ☑ NO
   ☐ YES - If yes, please explain the conflict: ______

STUDY INFORMATION

7. Study Title: An Analysis of Digital Forensic Units

8. Funding Source: Select all that apply:
   ☐ Sponsor-External Funds (Includes PRF, Kresge Trust and McCoy awards)
   ☐ Departmental Funding: __________
   ☑ Other Self-Funded: No Compensation

9. Anticipated Duration of Study: Please indicate when this project will end: August 20

10. Identify the expected age range(s) of participants to be included or targeted for this research and for which there is a reasonable expectation of enrollment into this research study.
    Check all that apply:
    ☐ under 18 years of age
    ☑ 18-64
    ☐ 65 and older

11. Identify where the research data collection will occur.
    Check all that apply:
    ☑ Purdue University, please identify campus: ______

Excerpt 2/3 v. 1/13
Elementary/Secondary School(s), please identify school(s): __________
Community Center, please identify: __________
Other University/College, please identify: __________
International Population(s) studied in their home country or within the US. Please identify the population(s) and the location of the data collection below. ALSO Section 1, International Research, of the non-exempt research application must be completed and submitted with this exemption request in addition to the required supplemental materials: __________
Internet
Subject's Home
Other location(s), please identify: Phone Survey of Law Enforcement units

12. Will the study collect data from focus group(s)?
☐ NO
☐ YES

13. Will elected or appointed public officials, or candidates for public office, participate in the research?
☐ NO
☐ YES – Identify which public office(s) participants either hold or are candidates for: __________

14. Will prisoners and/or individuals involved in court-ordered programs or community corrections (or their data and/or specimens) be participants in the research?
☐ NO
☐ YES – If yes, the research does not qualify for exemption. Please complete and submit a Non-Exempt Research Application for review by the convened board (aka full review).

15. Will the research involve surveys or interview procedures with participants under age 18?
☐ NO
☐ YES – If yes, the research does not qualify for exemption. Please complete and submit a Non-Exempt Research Application for review.

16. Will the research involve observations of participant behavior and the investigators will interact with those participants?
☐ NO
☐ YES – If yes and the participants will be under age 18, the research does not qualify for exemption. Please complete and submit a Non-Exempt Research Application for review.

STUDY PROCEDURES

17. Briefly state your research question using non-technical lay language that can be readily understood by someone outside the discipline.

Does having a cybercrime unit increase efficiency and effectiveness in law enforcement agencies?

18. Will survey procedures be used? Survey procedures CANNOT be used with children under 18 years of age.
☐ YES – Identify all surveys to be used AND submit them with this exemption request. Phone Interview and Online Questionnaire
☐ NO

19. Will interview procedures be used? Interview procedures CANNOT be used with children under 18 years of age.
☐ YES – Describe the interviews AND submit all interview questions/scripts with this exemption request. The phone interview will be used to gain general knowledge about the units. For example, when was the unit formed? What agencies are involved?
The online questionnaire will obtain numerical data. This data will include the number of digital devices the unit processed before and after the unit was created. The number of cases worked on before and after the unit was created.

☐ NO

20. Will educational tests be conducted?
☐ YES - Check the test categories to be used below and identify each test in the text box below. If the study tests do not fit into the categories below, the study does NOT qualify for this exemption.
☒ NO - Skip to question 21.
☐ Cognitive - Identify test(s) below and submit with exemption request.
☐ Diagnostic - Identify test(s) below and submit with exemption request.
☐ Aptitude - Identify test(s) below and submit with exemption request.
☐ Achievement - Identify test(s) below and submit with exemption request.
Identify the tests to be used:

21. Will observations of public behavior be made? Observational research involving sensitive aspects of a participant's behavior, or in settings where subjects have a reasonable expectation of privacy, does NOT qualify for exemption.
☐ YES - Describe the observations AND identify the venue(s) where data will be collected.
☒ NO

22. Will audio, visual or image (e.g., photograph) recordings be made?
☒ YES - Indicate below the type of recordings to be used. Check all that apply.
☐ NO - Skip to question 23.
☐ Audio recordings
☐ Video recordings
☐ Image recordings/photographs

Use of audio, visual or image (e.g., photographs) recordings are only permissible under these Exemptions if:

a. they are used for memory purposes ONLY to assist investigators in ensuring the accuracy of their collected data; AND
b. they will be destroyed once transcribed.

Explain in the text box below why the above-checked recording procedure(s) is necessary and how it meets both criteria a and b above.

The participant will be notified they are being recorded. The recordings will be used to assist with completing transcripts for the study and will help validate and verify information the interviewer received and noted down. The recording will be deleted from the computer it was stored on once completed.

23. Will any other procedures be used to collect data in the study? Please note, in most cases procedures that do not fall under these identified in questions 18-22 above do not qualify for exemption under these categories 2 and 3.
☐ YES - Identify all other procedures to be used in the study.
☒ NO

PRIVACY & CONFIDENTIALITY
24. Does this research involve the collection of any data that falls under any federal statute(s) requiring, without exception, that the confidentiality of the personally identifiable information will be maintained throughout the research and thereafter?

☐ YES - Identify the regulation(s): ______
☐ NO

25. Describe the provisions to protect the privacy interests of the participants. Consider the circumstances and nature of information to be obtained, taking into account factors (e.g., age, gender, ethnicity, education level, etc.) that may influence participants’ expectations of privacy.

The name of the agency and demographics such as what counties the unit serves will be gathered. This data will be kept confidential. The data will be de-identified and each agency will be given a random identifier. Only Dr. Kathryn Seifried-Spellar and Kathryn Garule will have access to the identifier key. The demographic information will be generalized and aggregated. For example, if the unit said they were located in West Lafayette and another unit said they were located in New York City, the aggregated and de-identified data would state a unit within a small town versus a unit within a larger metropolitan city.

26. Indicate below how the investigator will receive/record the research data.

☐ No identifiable data received – Skip to question 30.
☐ Coded data received; investigators have NO access to code key – Skip to question 30.
☐ Coded data will be received; investigators have access to code key
☒ Identifiable data received/recorded by investigators

27. Describe what provisions, if any, will be taken to maintain confidentiality of identifiable data (e.g., surveys, audio, video, etc.). Please state where the data will be stored, how long it will be kept and who will access it.

Only Dr. Kathryn Seifried-Spellar and Kathryn Garule will have access to the identifying data and the identifier key. The data will be kept on a personal computer and will be encrypted. The final data will be de-identified and aggregated.

28. Will identifiable data and/or coded (linked) data be made available to anyone other than the research team?

☒ NO
☐ YES - If yes, please identify to whom data will be made available and the reason for the disclosure. ______

29. Indicate below what will happen to the identifiable data at the end of the study.

☐ Identifiers permanently removed from the data and destroyed
☐ Recordings transcribed without identifiers and destroyed
☒ Identifiable or coded (that can be linked) data are retained

RECRUITMENT

30. Identify below all recruitment procedures and materials used in the study. Submit a copy of all materials or text summaries for phone calls and media advertisements.

☐ Face-to-face contact
☐ Flyer(s)
☐ Letter(s)
☒ Phone
☐ Email(s)
☐ Media Advertisement(s) – Indicate below the media outlet used
☐ newspaper
☐ radio
☐ television
31. Briefly describe how potential participants will be contacted and identify who will contact them. Kaelyn Guglielmi will send an email to the participants providing a brief description of the study. If the study is being completed and letting them know a phone call will be made in 3 days in order to discuss setting up a time for a phone interview if they wish to participate. A phone call will be made to both the commands of the unit and the administrative assistant to schedule the interview. The phone interview will be conducted. At the end of the interview, Kaelyn will let them know a follow-up questionnaire will be emailed to them by the end of the day. The questionnaire will be completed online and the participant will have a week to complete it. Should the participants need more time to answer the questionnaire, an additional week will be allowed.

32. Is participant contact information publicly available?
☐ NO
☐ YES - skip to question 35.

33. Will you obtain participant contact information from records?
☐ NO
☐ YES - Indicate record type below.
☐ Education records
☐ Employment records
☐ Medical records
☐ Other - Explain: ______

34. Explain how you will have permissible access to the records identified above. ______

COMPENSATION

35. Will you give the participants gifts, payments, compensation, reimbursement, or services in return for their participation in the research study? See guidance Compensation for Research Participation.
☐ NO - Skip to Principal Investigator's Assurance section.
☐ YES - Describe the compensation type (e.g., monetary, extra credit, etc.) and amount: ______

Extra credit – When extra credit is used as compensation for research participation, it cannot exceed 3% of the participant's grade. The investigator is obligated to make the class instructor aware of this limit and the requirement that students be offered an alternative non-research activity, comparable in time and effort, to earn a comparable amount of extra credit.

PRINCIPAL INVESTIGATOR'S ASSURANCE

As principal investigator of this study, I assure that the information supplied in this form and attachments are complete and correct. I have read the Researcher Responsibilities and will conduct this research in accordance with these requirements.

Principal Investigator's Signature: [Signature]
Date: 1/25/16

Submit this signed form and attachments to the Human Research Protection Program office either via hand copy or electronically. Forms received without signatures will be returned. A signed form and attachments can be submitted electronically as an email attachment to hrc@purdue.edu. If a signed form is submitted electronically, a paper copy need not be submitted.

Campus Address: Human Research Protection Program
U.S. Mail Address: Human Research Protection Program
YONG, 10th Floor, Rm. 1032
765-494-5942
irb@purdue.edu
Office Hours: M-F 8-11 am 1-5 pm
Purdue University
YONG, Rm. 1032
155 Grant Street
West Lafayette, IN 47906-2114

QUESTIONS? Call our office at 765-494-5942 or attend walk-in hours.
WALK-IN HOURS – Come speak to a Protocol Analyst
Monday 9:30 am - 11:30 am
Tuesday 2:00 pm - 4:00 pm
Thursday 9:30 am - 11:30 am
CHAPTER B. INFORMATION SHEET
What is the purpose of this study?
The purpose of this study is to examine different types of digital forensic units.

What will I do if I choose to be in this study?
If you choose to participate in this study, you will be interviewed via a telephone interview and you will receive, via email, and online questionnaire. Both the phone interview and the online questionnaire will be used to gather confidential data regarding your unit.

How long will I be in the study?
Most people take about 30 minutes to complete the telephone interview. After the telephone interview is completed, you will receive a follow-up online survey that takes approximately 15 minutes to complete. You will be given seven days to complete the online survey at your convenience if you wish to do so.

What are the possible risks or discomforts?
The risks to you are minimal. The phone interview will be recorded, but for memory purposes, in order to assist the researchers in ensuring the accuracy of their collected data. These recordings will be encrypted and only the investigators of this study will have access to them. Demographic information and other data regarding your unit will be collected. The data collected will be kept confidential in that only the researchers will know who completed the study. The data will be deidentified, generalized and aggregated so that your responses can not be linked back to you.

Are there any potential benefits?
There are no direct benefits to you. Eventually, we hope to publish the research results, and if you want to see them, you should send an email requesting information to the Principal Investigator at kspellar@purdue.edu.

Will I receive payment or other incentive?
Participants will not be compensated for their participation.

Will information about me and my participation be kept confidential?
The project's research records may be reviewed by Kathryn Seigfried-Spellar, Kaitlyn Gurule and by departments at Purdue University responsible for regulatory and research oversight. Only Dr. Kathryn Seigfried-Spellar and Kaitlyn Gurule will have access to the identifying data. However, the results will be deidentified and aggregated, so that your responses to this study can not be linked back to you. The data will be stored electronically in an encrypted format and will be used only for research purposes.
Exemption Granted Granted on 29-FEB-2016

What are my rights if I take part in this study?

Your participation in this study is voluntary. You may choose not to participate or, if you agree to participate, you can withdraw your participation at any time without penalty or loss of benefits to which you are otherwise entitled.

Who can I contact if I have questions about the study?

If you have questions, comments or concerns about this research project, you can talk to one of the researchers. Please contact Kaitlyn Gurule at (505) 273-4075 or if necessary Kathryn Seigfried-Spellar at (765) 494-2439.

If you have questions about your rights while taking part in the study or have concerns about the treatment of research participants, please call the Human Research Protection Program at (765) 494-5942, email (irb@purdue.edu) or write to:

Human Research Protection Program - Purdue University
Ernest C. Young Hall, Room 1032
155 S. Grant St.
West Lafayette, IN 47907-2114

Do you agree to participate in this study?

Agree  Do Not Agree
CHAPTER C. PHONE INTERVIEW QUESTIONS
Phone Interview Survey Questions

1. What is the name of your digital forensics unit?
2. Where is your unit located?
3. What year was your unit established?
4. Primarily, which types of cases does the unit work?
   1. Federal
   2. State
   3. Local
5. Did the unit receive grant funding to establish the unit? Yes or No?
   1. From which agency did you receive funding?
   2. Have you received any funding since the unit’s creation?
   3. From which agency did you receive funding?
6. What counties or populations are you serving?
7. Is your unit multi-agency? (Multiple law enforcement agencies, universities, prosecutor’s office, etc.)
   1. Can you list them?
8. How many personnel are in your unit?
   1. How many of those personnel are sworn law enforcement officers?
   2. How many Law Enforcement officers from this agency are a part of the unit?
   3. Who commands the unit?
9. How many of your unit personnel are certified digital forensics examiners?
   1. What certifications do they have?
10. Are specific people assigned to specific roles for digital forensics? (e.g., Mobile forensics investigator, network forensics investigator)
11. What were the reasons/goals for creating the unit?
   1. Have you met your goals?
   2. Do you believe the unit has been successful? Why?
   3. Are there new or additional goals?
12. Did your agency have a backlog prior to establishing the unit? If so, how far back was the backlog?
   1. Does your unit have a backlog after (as of today’s date) the unit was created? If so, how far back was the backlog?
13. Does your unit focus on specific types of crimes? If so, which ones?
14. What digital forensic tools does your unit use?
15. Do you process all of your digital evidence within the unit?
16. Are digital evidence resources shared among all agencies within the unit?
   1. Are the resources paid for by all agencies involved?
   2. Are you finding it more cost effective to share resources?
17. Do you have standard guidelines you follow for a digital forensics investigation?
   1. What are those standards?
   2. Is your unit ASCLD certified?
18. Does your unit offer mental health counseling for child pornography related cases?
   1. Do you rotate your personnel in and out of the unit?
   2. How does your personnel deal with seeing CP?
19. Would you recommend for other agencies to create a similar unit?
20. Is there anything else you think my analysis should consider?
21. Do you have any follow up questions for me?
CHAPTER D. ONLINE QUESTIONNAIRE
Online Questionnaire - Specialized

The following questions will be used in an analysis of specialized digital forensic units. The data obtained will be used to determine if specialized digital forensic units operate more efficiently and effectively than non-specialized units. The survey will take approximately 10-15 minutes to complete. The data collected will be kept confidential.

Please answer the questions to the best of your ability. If possible, exact values for the numerical data would be best. Please answer the questions as of today’s date unless specified otherwise.

1. What is the name of your digital forensics unit?
2. Where is your unit located?
3. What year was your unit established?
4. Out of a total of 100%, approximately what percentage of your unit’s cases are Federal, State, and Local?
5. To date, which counties has your unit served?
6. How many cases involving digital evidence did the unit work PRIOR to opening the specialized unit?
7. To date, how many cases involving digital evidence has the unit worked SINCE the specialized unit was created?
8. Do you process all of your digital evidence within the unit?
9. Out of 100%, what percentage of your unit’s time is spent as a digital forensic examiner vs. investigator for cases involving digital evidence?
10. What types of digital forensics does the unit conduct? Select all that apply.
   a. Computer forensics (dead-box forensics, hard drives)
   b. Mobile forensics
   c. Network forensics
   d. Malware forensics
   e. Video forensics
   f. Other
11. Which of these types of digital forensics is most prevalent in your unit?
   a. Computer forensics (dead-box forensics, hard drives)
   b. Mobile forensics
   c. Network forensics
   d. Malware forensics
   e. Video forensics
   f. Other
12. Approximately, how many of the following devices did the unit successfully analyze PRIOR to creating the unit?
   a. Computer Hard Drives
   b. Mobile Phones
   c. USB Drives
   d. Kindles, iPads, and other tablets
   e. Gaming Consoles (Xbox, PlayStation)
13. Approximately, how many of the following devices did the unit successfully analyze AFTER (as of today’s date) the unit was created?
   a. Computer Hard Drives
   b. Mobile Phones
   c. USB Drives
   d. Kindles, iPads, and other tablets
   e. Gaming Consoles (Xbox, PlayStation)
   f. Other

14. What is the average volume or storage capacity of digital evidence processed PRIOR to opening the unit (e.g., 160MB, 32GB, 4TB)?

15. What is the average volume or storage capacity of digital evidence processed AFTER (as of today’s date) opening the unit (e.g., 160MB, 32GB, 4TB)?

16. What was the average time spent on a case PRIOR to opening the unit?
   a. Less than a week
   b. Less than a month
   c. Less than six months
   d. Less than a year
   e. More than 1 year

17. What was the average time spent on a case AFTER (as of today’s date) opening the unit?
   a. Less than a week
   b. Less than a month
   c. Less than six months
   d. Less than a year
   e. More than 1 year

18. Out of 100%, what percentage of your unit’s cases that involve digital evidence are the following:
   a. Child pornography
   b. Drug
   c. Homicide
   d. Robbery
   e. Other

19. How many NCMEC/ICAC leads did the unit receive PRIOR to creating the unit?
20. How many NCMEC/ICAC leads has the unit received SINCE the unit was created?
21. How many IC3 reports did the unit submit PRIOR to creating the unit?
22. How many IC3 reports has the unit submitted SINCE the unit was created?
Online Questionnaire – Non-Specialized

The following questions will be used in an analysis of specialized digital forensic units. The data obtained will be used to determine if specialized digital forensic units operate more efficiently and effectively than non-specialized units. The survey will take approximately 10-15 minutes to complete. The data collected will be kept confidential.

Please answer the questions to the best of your ability. If possible, exact values for the numerical data would be best. Please answer the questions as of today’s date unless specified otherwise.

1. What is the name of your digital forensics unit?
2. Where is your unit located?
3. What year was your unit established?
4. Out of a total of 100%, approximately what percentage of your unit’s cases are Federal, State, and Local?
5. To date, which counties has your unit served?
6. How many cases involving digital evidence did the unit work?
7. Do you process all of your digital evidence within the unit?
8. Out of 100%, what percentage of your unit’s time is spent as a digital forensic examiner vs. investigator for cases involving digital evidence?
9. What types of digital forensics does the unit conduct? Select all that apply.
   a. Computer forensics (dead-box forensics, hard drives)
   b. Mobile forensics
   c. Network forensics
   d. Malware forensics
   e. Video forensics
   f. Other
10. Which of these types of digital forensics is most prevalent in your unit?
    a. Computer forensics (dead-box forensics, hard drives)
    b. Mobile forensics
    c. Network forensics
    d. Malware forensics
    e. Video forensics
    f. Other
11. Approximately, how many of the following devices does the unit successfully analyze?
    a. Computer Hard Drives
    b. Mobile Phones
    c. USB Drives
    d. Kindles, iPads, and other tablets
    e. Gaming Consoles (Xbox, PlayStation)
    f. Other
12. What is the average volume or storage capacity of digital evidence processed by the unit (e.g., 180MB, 32GB, 4TB)?
13. What is the average time spent on a case within the unit?
a. Less than a week
b. Less than a month
c. Less than six months
d. Less than a year
e. More than 1 year

14. Out of 100%, what percentage of your unit’s cases that involve digital evidence are the following:
   a. Child pornography
   b. Drug
   c. Homicide
   d. Robbery
   e. Other

15. How many NCMEC/ICAC leads does the unit receive?

16. How many IC3 reports does the unit submit?